

## REMARKS

Claims 54-150 have been copied in the present continuation application under the provisions of 37 C.F.R. §§ 1.604 and 1.607 to invoke an interference. Claims 54-150 were originally copied in parent U.S. Patent Application No. 09/321,386 filed May 27, 1999 but have been moved to the present continuation application as per the Examiner's request. Claims 55-63, 67-74, 77-78, 81-82, 86-87 have been copied in this present continuation application prior to canceling the same claims in Application No. 09/321,386 so as to put that application into better form for declaration of an interference.

Claim 54 is copied substantially verbatim from U.S. Patent No. 6,292,569 (hereinafter "Shear '569"), granted September 18, 2001, to Shear et al. Claim 54 corresponds to claim 1 of Shear '569.

Claims 55-95 are copied substantially verbatim from U.S. Patent Application No. 08/848,077, Publication No. 2001/0042043, published November 15, 2001, for Shear et al. (hereinafter "Shear Appl. '077"). Claims 55-95 correspond to claims 1-2, 7, 10, 13, 19-29, 32, 35-39, 41, 44-46, 55, 65-67, 69-70, 73-74, 79, 80-81, 95-98, and 118, respectively, of the '077 Patent Application. A one-to-one correspondence between the copied claims and the claims of the Shear Appl. '077 is shown in Table 1 below.

Claims 96-110 are copied substantially verbatim from U.S. Patent Application No. 09/925,072, Publication No. 2002/0023214, published February 21, 2002, for Shear et al. (hereinafter "Shear Appl. '072"). Claims 96-110 correspond to claims 6, 9, 10, 11, 15, 19, 21, 22, 27, 30, 31, 32, 36, 40, and 42 of the '072 Patent Application. A one-to-one correspondence between the claims and the claims of the Shear Appl. '072 is shown in Table 2 below.

Claims 111-116 are copied substantially verbatim from U.S. Patent Application No. 09/948,806, Publication No. 2002/0048369, published April 25, 2002, for Ginter et al. (hereinafter "Ginter Appl. '806"). Claims 111, 112, 113, 114, 115, and 116 correspond to Ginter Appl. '806 claims 1, 2, 3, 4, 7, and 8, respectively.

Claims 117-144 are copied substantially verbatim from U.S. Patent Application No. 09/764,370, Publication No. 2002/0112171, published August 15, 2002, for Ginter et al.



(hereinafter "Ginter Appl. '370"). Added claims 117-144 correspond to Ginter Appl. '370 claims 1, 13-16, 36-37, 45, 49, 55, 58, 60, 64-67, 70-76, 79-81, and 89-90. A one-to-one correspondence between the claims and the Ginter Appl. '370 claims is shown in Table 3 below.

Claims 145-148 are copied substantially verbatim from U.S. Patent No. 6,427,140, granted July 30, 2002, to Ginter et al. (hereinafter "Ginter '140). Claims 145, 146, 147, and 148 correspond to Ginter '140 claims 1, 10, 24, and 29, respectively.

Claim 149 is copied substantially verbatim from U.S. Patent No. 6,389,402, granted May 14, 2002, to Ginter et al. (hereinafter "Ginter '402). Claim 149 corresponds to Ginter '402 claim 1.

Claim 150 is copied substantially verbatim from U.S. Patent No. 6,363,488, granted March 26, 2002, to Ginter et al. (hereinafter "Ginter '488). Claim 150 corresponds to Ginter '488 claim 1.



Claim No.	Shear Appl. '077 Claim No.	Claim No.	Shear Appl. '077 Claim No.
55	1	76	41
56	2	77	44
57	7	78	45
58	10	79	46
59	13	80	55
60	19	81	65
61	20	82	66
62	21	83	67
63	22	84	69
64	23	85	70
65	24	86	73
66	25	87	74
67	27	88	79
68	28	89	80
69	29	90	81
70	32	91	95
71	35	92	96
72	36	93	97
73	37	94	98
74	38	95	118
75	39		

Table 1



<b>Claim No.</b>	<b>Shear Appl. '072 Claim No.</b>
96	6
97	9
98	10
99	11
100	15
101	19
102	21
103	22
104	27
105	30
106	31
107	32
108	36
109	40
110	42

Table 2



<b>Claim No.</b>	<b>Ginter Appl. '370 Claim No.</b>
117	1
118	13
119	14
120	15
121	16
122	36
123	37
124	45
125	49
126	55
127	58
128	60
129	64
130	65
131	66
132	67
133	70
134	71
135	72
136	73
137	74
138	75
139	76
140	79
141	80
142	81
143	89
144	90

Table 3

In accordance with 37 C.F.R. §§ 1.604 and 1.607, the copied claims may be specifically applied to Applicants' disclosure as follows:



Copied Claim from Shear '569	Applicants' Disclosure
54. A security method comprising:	Applicants disclose that a general set of control data comprises a security control element which defines a security procedure which has to be carried out before usage of a data object. (p.4, ll.17-19).



(a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class;

- Applicants disclose encrypting (i.e., digitally signing) control elements and a data object (i.e., a first load module) (p.4, ll.27-28; p.12, ll.15-18) to create a secure data package ready for transfer to a user (p.5, ll.7-10). Applicants disclose that usage control elements define a variety of usages of the data object, for example the kind of user, allowed operations, and security modules required for use of the data object on a user's data processor (i.e., the digital signature designates the load module for use by a device class). (p.4, ll.11-15; p.18, ll.1-5).
- Applicants further disclose that the security of a data package can be improved by using a sophisticated encryption algorithm like RSA (p.21, ll.18-20) or other encryption and key methods (p.12, ll.15-18). Such usage is recognized as applying a digital signature. *See e.g.*, Shear '569, col.13, ll.8-10 and 25-26 (Different digital signatures can be made by using different encryption algorithms. Two digital signature algorithms in widespread use today include RSA (a public key cryptosystem) and digital signature algorithm (DSA)).
- Applicants disclose that the user's data processor is a general or special purpose processor (p.17, ll.2-3), data objects include books, films, video, news, music, software, games, etc. (p.2, ll.3-4), and the data object owner may want to have control over how, when, where, and by whom his property is used (p.2, ll.20-21). Applicants further disclose that object security is extensible in the sense that multiple levels of security can be applied, being dependent on the encryption/key method which is implemented in the security modules. (p.23, ll.26-29). Thus, Applicants disclose that a variety of data objects (i.e., load modules) can be designated for use by data processors having certain required security modules (i.e., a device class).
- Therefore, Applicants disclose digitally signing (i.e., encrypting) a first load module (i.e., a data object such as a digital image or a video file) with a first digital signature designating the first load module for use by a first device class (i.e., the encrypted control/usage elements require the user's data processor to have certain required security modules in order to use the data object).



(b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class;

- See (a) above regarding digitally signing a load module and designating a device class.
- Applicants disclose the secure transfer of two different examples of data objects, a digital image (i.e., a first load module) and a video film (i.e., a second load module), requiring different security treatment with different security modules by a user's data processor prior to usage of the data objects (i.e., designating load modules for use by devices having different tamper resistance and/or work factors). (p.20, l.5-p.23, l.2).
- Applicants disclose that the general set of control data associated with a data object comprises an identifier, which uniquely identifies the general set of control data. The whole set of control data and the data object may be encrypted (i.e., digital signature of a second load module can be different from a digital signature of a first load module). (p.4, ll.19-28).
- Applicants disclose that a user program comprising a usage manager module controls the usage of a data object in accordance with the control data. The user program comprises one or more security modules (i.e., user device level of security, or user device tamper resistance and/or work factor). (p.17, ll.15-20). The usage manager module applies the security modules which are necessary to use a data object. If the proper security modules are not available for a particular data object, the usage manager module will not permit usage of the data object (i.e., a second device class may have a tamper resistance and/or work factor different from the tamper resistance and/or work factor of the first device class). (p.18, ll.1-5).
- Therefore, Applicants disclose digitally signing a second load module (e.g., a video file or a digital image) with a second digital signature different from the first digital signature (i.e., encrypted unique control data), the second digital signature designating the second load module for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class (i.e., encrypted control/usage elements can require the user's data processor to have different security modules in order to use different data objects).



(c) distributing the first load module for use by at least one device in the first device class; and	Applicants disclose that a secured data package, for example a digital image (i.e., a first load module) is transferred/distributed to a user for use on the user's data processor having certain required security modules (i.e., distributed for use by at least one device in a first device class). (p.5, ll.17-19; p.20, l.5-p.22, l.12).
(d) distributing the second load module for use by at least one device in the second device class.	Applicants disclose that a secured data package, for example a video film (i.e., a second load module) is transferred/distributed to a user's data processor which must have a different set of security modules, as compared to the example in (c) involving a digital image, in order for the video film to be used (i.e., distributed for use by at least one device in a second device class). (p.5, ll.17-19; p.22, l.13-23). <i>See</i> (b) above.



Copied Claim From Shear Appl. '077	Applicants' Disclosure
55. An electronic appliance including:	Applicants disclose a data processor (i.e., an electronic appliance). (p.8, l.25-p.9, l.9; p.17, ll.1-12).
a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and	<ul style="list-style-type: none"> <li>Applicants disclose a data processor including a CPU, a bus, and a bulk storage device (i.e., a disk use arrangement) for data object usage (i.e., reading information from), and data object packaging (i.e., writing information to) related to storage media such as CD-ROM (i.e., substantially the same as a digital versatile disk optical storage medium). (p.8, l.25-p.9, l.9; p.11, l.21-p.12, l.22; p.17, ll.1-12; p.19, l.1-p.20, l.4).</li> <li>These disk functions can be combined into one electronic appliance since Applicants disclose the use of a broker who receives and transfers secure data packages. (p.8, ll.9-17).</li> <li>Therefore, Applicants disclose a disk use arrangement (i.e., a data processor including a CPU, a bus, and a bulk storage device) that is capable of reading information from and writing information to (i.e., data object usage and data object packaging) a digital versatile disk optical storage medium (i.e., storage media such as CD-ROM).</li> </ul>



a secure node coupled to the disk use arrangement, the secure node providing at least one rights management process.

- Applicants disclose that the user's data processor is a general or special purpose processor (p.17, ll.2-3) requiring certain security modules for usage of the data object (i.e., a secure node) in accordance with control/usage data (i.e., providing a rights management process). (p.17, ll.15-16; p.18, ll.3-5; p.19, l.1-p.20, l.4).
- Applicants disclose that if the proper format and security modules are not available for a particular data object, usage is not permitted. (p.18, ll.3-5).
- Applicants further disclose that the user program can have code which controls use of the program by password. (p.18, ll.13-14).
- Applicants further disclose that the data object is never stored in native format in user accessible storage. (p.18, ll.22-24).
- Applicants further disclose that the data provider's data processor is considered secure. (p.9, ll.8-9).
- Therefore, Applicants disclose a secure node coupled to the disk use arrangement (i.e., a data processor with required security) that provides a rights management process (i.e., data object usage according to control/usage data).



Copied Claim From Shear Appl. '077	Applicants' Disclosure
56. An electronic appliance including:	<i>See Claim 55 above.</i>
a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and	<i>See Claim 55 above.</i>
at least one processing arrangement coupled to the disk use arrangement, the processing arrangement selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.	Applicants disclose a user program stored in a user's data processor (i.e., a processing arrangement coupled to the disk use arrangement) that controls the usage of a data object (i.e., information recorded on a storage medium) in accordance with control data (i.e., control information) for example requiring a security procedure (i.e., class of the appliance) and/or a certain kind of user (i.e., the user of the appliance). (p.17, ll.1-16; p.4, ll.11-20; p.19, l.1-p.20, l.4).



Copied Claim From Shear Appl. '077	Applicants' Disclosure
57. In an appliance capable of using digital versatile disks, a method including the following steps:	<i>See Claim 56 above.</i>
at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and	<i>See Claim 56 above.</i>
selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.	<i>See Claim 56 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
58. An electronic appliance including:	<i>See Claim 55 above.</i>
a disk use arrangement for reading information from a digital versatile disk optical storage medium; and	<i>See Claim 55 above.</i>
at least one processing arrangement coupled to the disk use arrangement, the processing arrangement protecting information read from the storage medium.	<ul style="list-style-type: none"> <li>• <i>See Claims 55 and 56 above.</i></li> <li>• Applicants disclose a user program stored in a user's data processor that controls the usage of a data object (i.e., information read from a storage medium) in accordance with control data (i.e., protecting the information). (p.17, ll.1-16; p.4, ll.11-20).</li> <li>• Applicants further disclose that the data object is never stored in native format in user accessible storage. (p.18, ll.22-24).</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
59. In an electronic appliance, a method including the following steps:	<i>See Claim 58 above.</i>
reading information from a digital versatile disk optical storage medium; and	<i>See Claim 58 above.</i>
protecting the information read from the optical storage medium.	<i>See Claim 58 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
60. An electronic appliance including:	<i>See Claim 56 above.</i>
a disk use arrangement for using information stored, or to be stored, on a digital versatile disk optical storage medium; and	<i>See Claim 56 above.</i>
at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement treating the storage medium and/or information obtained from the storage medium differently depending on the geographical and/or jurisdictional context of the appliance.	<ul style="list-style-type: none"> <li>• <i>See Claim 56 above.</i></li> <li>• Applicants disclose a user program stored in a user's data processor (i.e., a rights management arrangement coupled to the disk use arrangement) that controls the usage of a data object (i.e., information obtained from a storage medium) in accordance with control data that can include a geographical area for usage and the kind of user allowed (i.e., the geographical and/or jurisdictional context). (p.17, ll.1-16; p.4, ll.11-20).</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
61. In an electronic appliance, a method including the steps of:	<i>See Claim 60 above.</i>
reading information from at least one digital versatile disk; and	<i>See Claim 60 above.</i>
performing at least one rights management operation based at least in part on the geographical and/or jurisdictional context of the appliance.	<i>See Claim 60 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
62. An electronic appliance including:	<i>See Claim 60 above.</i>
a disk use arrangement for using at least one secure container stored on a digital versatile disk optical storage medium; and	<ul style="list-style-type: none"> <li>• <i>See Claim 60 above.</i></li> <li>• Applicants disclose a data processor including a data packaging program that can store a secure data package (i.e., a secure container) on storage media such as CD-ROM for distribution. (p.12, ll.19-22).</li> </ul>
at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement processing the secure container.	<ul style="list-style-type: none"> <li>• <i>See Claim 60 above.</i></li> <li>• Applicants disclose a data processor including a user program for controlling the usage of a data object in the secure data package (i.e., processing the secure container). (p.17, ll.15-16; p.19, l.1-p.20, l.4).</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
63. In an electronic appliance, a method including the following steps:	<i>See Claim 62 above.</i>
reading at least one secure container from at least one digital versatile disk; and	<i>See Claim 62 above.</i>
performing at least one rights management operation on the secure container.	<i>See Claim 62 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
64. An electronic appliance including:	<i>See Claim 62 above.</i>
at least one rights management arrangement for generating and/or modifying at least one secure container for storage onto a digital versatile disk optical storage medium.	<i>See Claim 62 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
65. In an electronic appliance, a method including the step of performing at least one rights management operation on at least one secure container for storage onto a digital versatile disk optical storage medium.	<i>See Claim 62 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
66. A digital versatile disk use system and/or method characterized in that the system and/or method uses at least one secure container.	<i>See Claim 62 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
67. An electronic appliance including:	<i>See Claim 55 above.</i>
a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and	<i>See Claim 55 above.</i>



a secure arrangement that securely manages information on the storage medium such that at least a first portion of the information may be used on at least a first class of appliance while at least a second portion of the information may be used on at least a second class of appliance.

- See Claims 55 and 56 above.
- Applicants disclose variable object control and/or security in which variation of object control and/or security can be applied to a particular object by creating a control data format with control elements defining the control and/or security variation and the circumstances in which the variation is applied. (p.23, l.3-p.24, l.9).
- Applicants disclose an example of a broker allowing students to print a particular article for free but requiring business users to pay. (p.23, ll.9-12).
- Applicants disclose an example of a broker applying minimal security to a collection of current news articles (i.e., a first portion of information may be used on a first class of appliance) but applying tight security to encyclopedia and text books (i.e., a second portion of information may be used on a second class of appliance). (p.23, ll.23-25).
- Applicants further disclose that object security is extensible in the sense that multiple levels of security can be applied. (p.23, ll.26-30).
- Applicants further disclose composite data objects with constituent objects retaining their original control data to control usage. (p.24, ll.27-31).
- See Shear et al., Pub. No. US 2001/0042043, para.34 (class of appliance refers to, for example, type of appliance, available resources and/or rights).



<b>Copied Claim From Shear Appl. '077</b>	<b>Applicants' Disclosure</b>
68. In an electronic appliance, a method including the following steps:	<i>See Claim 67 above.</i>
reading information from and/or writing information to at least one digital versatile disk optical storage medium;	<i>See Claim 67 above.</i>
using at least a first portion of the information on at least a first class of appliance; and	<i>See Claim 67 above.</i>
using at least a second portion of the information on at least a second class of appliance.	<i>See Claim 67 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>69. A system including first and second classes of electronic appliances each including a secure processing arrangement, the first appliance class secure arrangement securely managing and/or using at least a first portion of the information, the second appliance class secure arrangement securely managing and/or using at least a second portion of the information.</p>	<ul style="list-style-type: none"> <li>• See Claim 67 above.</li> <li>• Applicants disclose a data provider's data processor and a user's data processor, in which usage of a data object will not be permitted without the proper format and security modules. (p.18, ll.1-5).</li> <li>• Applicants further disclose a broker's data processor (p.8, ll.9-17), a bulletin board service's data processor (p.20, ll.9-11), and a stock trading company's data processor (p.26, ll.25-27).</li> <li>• Thus, a system including first and second classes is disclosed.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
70. In a system including first and second classes of electronic appliances each including a secure arrangement, a method comprising:	<i>See Claim 69 above.</i>
(a) securely managing and/or using at least a first portion of the information with the first appliance class secure arrangement, and	<i>See Claim 69 above.</i>
(b) securely managing and/or using at least a second portion of the information with the second appliance class secure arrangement.	<i>See Claim 69 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
71. An electronic appliance including:	<i>See</i> Claim 55 above.
a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and	<i>See</i> Claim 55 above.
a secure arrangement that securely stores and/or transmits information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.	<ul style="list-style-type: none"> <li>• <i>See</i> Claims 55 and 56 above.</li> <li>• Applicants disclose a data processor (i.e., a secure arrangement) that controls the usage of a data object in accordance with control data (i.e., information associated with managing content recorded on the storage medium) that can include a claim to payment, number of usages (i.e., auditing), and allowed operations (i.e., controlling). (p.17, ll.15-16; p.4, ll.11-20; p.19, l.1-p.20, l.4).</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
72. In an electronic appliance, a method including the following steps:	<i>See Claim 71 above.</i>
reading information from and/or writing information to at least one digital versatile disk optical storage medium; and	<i>See Claim 71 above.</i>
securely storing and/or transmitting information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.	<i>See Claim 71 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
73. An electronic appliance including:	<i>See Claim 71 above.</i>
a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium;	<i>See Claim 71 above.</i>
a cryptographic engine coupled to the disk use arrangement, the engine using at least one cryptographic key; and	<ul style="list-style-type: none"> <li>• Applicants disclose encryption modules and security modules (i.e., a cryptographic engine) are part of a data processor's (i.e., a disk use arrangement) program. (p.9, ll.15-18; p.17, ll.17-20).</li> <li>• Applicants disclose that a security module containing an encryption algorithm involving keys, such as RSA, could be used. (p.21, ll.17-31).</li> </ul>
a secure arrangement that securely updates and/or replaces at least one cryptographic key used by the cryptographic engine to at least in part modify the scope of information usable by the appliance.	<ul style="list-style-type: none"> <li>• <i>See Claim 67 above.</i></li> <li>• Applicants disclose that variation of object security (i.e., update and/or replacement of keys to modify information usage) can be applied to a particular object by creating a control data format with control elements defining the security variation and the circumstances in which the variation is applied. (p.23, ll.16-26).</li> <li>• Thus, it is inherent that an arrangement that updates and/or replaces a cryptographic key to modify the scope of information usable by the appliance is disclosed.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
74. A method of operating an electronic appliance including:	<i>See Claim 73 above.</i>
writing information onto and/or reading information from a digital versatile disk optical storage medium;	<i>See Claim 73 above.</i>
using at least one cryptographic key in conjunction with said information; and	<i>See Claim 73 above.</i>
securely updating and/or replacing at least one cryptographic key used by the cryptographic engine key used by the cryptographic engine to at least in part modify the scope of information useable by the appliance.	<i>See Claim 73 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
75. A digital versatile disk appliance characterized in that at least one cryptographic key used by the appliance is securely updated and/or replaced to at least in part modify the scope of information that can be used by the appliance.	<i>See Claim 73 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>76. An electronic appliance having a class associated therewith, characterized in that at least one cryptographic key set used by the appliance class is selected to help ensure security of information released from at least one digital versatile disk.</p>	<ul style="list-style-type: none"> <li>• Applicants disclose that a security module containing an encryption algorithm involving keys, such as RSA, could be used. (p.21, ll.17-31).</li> <li>• Applicants further disclose that object security is extensible in the sense that multiple levels of security can be applied. (p.23, ll.26-30).</li> <li>• Thus, it is inherent that a cryptographic key set used by the appliance class is disclosed.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
77. In an electronic appliance including a disk use arrangement, a method comprising:	<i>See Claim 55 above.</i>
reading information from at least one digital versatile disk optical storage medium; and	<i>See Claim 55 above.</i>
persistently protecting at least some of the read information through at least one subsequent editing and/or production process.	<ul style="list-style-type: none"> <li>• Applicants disclose that when a user has finished usage of the data object, the user program restores the data package in the secure form (the data object and the usage elements are reconcatenated and reencrypted). (p.8, ll.20-21; p.19, l.31-p.20, l.3).</li> <li>• Applicants disclose a usage condition can be to not permit further cutting or pasting. (p.12, ll.25-29).</li> <li>• Applicants disclose a security module may implement an authorization process in which each usage of the data object requires a dialup to the data processor of the data object provider, resulting in a permanent data object security. (p.22, ll.1-12).</li> <li>• Applicants disclose composite data objects comprising constituent objects with control data controlling each constituent object usage and control data controlling the composite object usage. Constituent objects may be combined or separately used while retaining their original control data (i.e., protecting the information through an editing and/or production process). (p.24, l.11-p.25, l.3).</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
78. In an electronic appliance, a method including the following steps:	<i>See Claim 67 above.</i>
reading information from and/or writing information to at least one digital versatile disk optical storage medium; and	<i>See Claim 67 above.</i>
securely managing information on the storage medium, including the step of using at least a first portion of the information on at least a first class of appliance, and using at least a second portion of the information on at least a second class of appliance.	<i>See Claim 67 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>79. A method of providing copy protection and/or use rights management of at least one digital property content and/or secure container to be stored and/or distributed on a digital versatile disk medium, comprising the step(s) of:</p>	<p>Applicants disclose a method for managing a data object, securely packaged by encryption, to be stored and/or distributed on a storage medium such as CD-ROM. (p.7, l.23-p.8, l.17; p.12, ll.19-22).</p>
<p>providing a set of use control(s) within a cryptographically encapsulated data structure having a predetermined format, the data structure format defining at least one secure software container for providing use rights information for digital property content to be stored on the digital versatile disk medium.</p>	<ul style="list-style-type: none"> <li>• Applicants disclose control data comprising usage control elements (i.e., use controls) as part of an encrypted data object package (i.e., a data structure). (p.4, ll.11-13; p.5, ll.7-10).</li> <li>• The control data may have a format that is unique or defined according to a standard. (p.11, ll.14-19).</li> <li>• Applicants disclose that the control data is concatenated with a copy of the data object. At least the usage control elements and the data object are encrypted so that the data object cannot be used without a user program which performs the usage control and which decrypts the data object (i.e., cryptographically encapsulated), and alternatively, the whole set of control data and the data object may be encrypted (i.e., cryptographically encapsulated). (p.4, ll.21-28; FIGS.9&amp;17).</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>80. An arrangement for implementing a rights management system for controlling copy protection, use and/or distribution rights to multi-media digital property content stored or otherwise contained on a digital versatile disk, comprising:</p>	<p><i>See Claim 79 above.</i></p>
<p>an encrypted data structure defining a secure information container stored on an optical disk medium, the encrypted data structure including and/or referencing at least one content object and at least one control object associated with the content object, said content object comprising digital property content and said control object comprising rules defining use rights to the digital property content.</p>	<p><i>See Claim 79 above.</i></p>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>81. A rights management system for providing copy protection, use and/or distribution rights management for multimedia digital property content stored or otherwise contained on a digital versatile disk for access by an optical disk player device that uses digital property content stored on said optical disk medium, wherein said appliance includes a microprocessor controller for decrypting and using control rules and other selected encrypted information content encapsulated in the secure container by using a prescribed cryptographic key and applying said decrypted control rules to regulate use in accordance with control information contained within said control rules, so as to facilitate management of a diverse set of use and/or distribution rights which may be specific to different users and/or optical disk appliances, the system including:</p>	<ul style="list-style-type: none"> <li>• See Claim 79 above.</li> <li>• Applicants disclose that a security module containing an encryption algorithm involving keys, such as RSA, can be used. (p.21, ll.17-31).</li> </ul>
<p>an optical disk medium having stored thereon an encrypted data structure defining a secure information container, the encrypted data structure comprising and/or referencing at least one content object and at least one control object, said content object comprising digital property content, said control object comprising rules defining use rights associated with the digital property.</p>	<p>See Claim 79 above.</p>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>82. A method for providing copy protection, use and distribution rights management of multi-media digital property stored on and/or distributed via digital versatile disk, said optical disk medium having stored thereon an encrypted data structure defining a secure container for housing rights and/or copy protection information pertaining to digital property content stored on the optical disk, wherein an optical disk player appliance for using digital property content stored on an optical disk must utilize a prescribed secure cryptographic key or set of keys to use the secure container, said data structure comprising one or more content objects comprising digital property content and one or more control objects comprising a set of rules defining use right to digital property, comprising the steps of:</p>	<p><i>See Claims 79 and 81 above.</i></p>
<p>(a) decrypting control rules and other selected encrypted information content encapsulated in the secure container using one or more cryptographic keys; and</p>	<p><i>See Claims 79 and 81 above.</i></p>



<p>(b) applying decrypted control rules to regulate use and/or distribution of digital property content stored on the optical disk in accordance with control information contained within the control rules, so as to provide customized use and/or distribution rights that are specific to different optical disk user platforms and/or optical disk appliances.</p>	<ul style="list-style-type: none"> <li>• See Claims 79 and 81 above.</li> <li>• Applicants disclose a data package may include control data which is specifically adapted to a user. (p.7, 1.28-p.8, 1.8).</li> <li>• Applicants disclose that the data provider may define any number of control elements to represent his predetermined conditions of usage of the data object (p.11, 11.3-4), including kind of user and security procedures required. (p.4, 11.11-20).</li> <li>• Thus, it is inherent that rights that are specific to different “optical disk user platforms and/or optical disk appliances” is disclosed.</li> </ul>
---	---



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>83. A rights management system for providing copy protection, use and/or distribution rights management of digital property stored or otherwise contained on a digital versatile disk, comprising:</p>	<p><i>See Claim 79 above.</i></p>
<p>a secure container means provided on an optical disk medium for cryptographically encapsulating digital property content stored on the optical disk, said container means comprising a content object means for containing digital property content and a control object means for containing control rules for regulating use and/or distribution of said digital property content stored on the optical disk.</p>	<p><i>See Claim 79 above.</i></p>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>84. In a system including plural electronic appliances at least temporarily connected to one another, a rights authority broker that determines what appliances are connected and specifies at least one rights management context depending on said determination.</p>	<ul style="list-style-type: none"> <li>• Applicants disclose a system in which data processors (i.e., plural electronic appliances) are connected to one another. (p.19, ll.1-12).</li> <li>• Applicants disclose that an object author may send his data object to a broker (p.8, ll.9-17) who distributes the data object to users.</li> <li>• Applicants disclose that a user can be required to comply with a request for authorization process through the broker (p.22, ll.1-12) at which time the broker can check parameters including that the object has not already been loaded (p.24, ll.1-2) utilizing a user set of control data (p.8, ll.1-8).</li> <li>• Applicants disclose that the data provider (or broker) may define any number of control elements to represent his predetermined conditions of usage of the data object (p.11, ll.3-4), including kind of user and security procedures required. (p.4, ll.11-20).</li> <li>• Thus, it is inherent that a broker could determine what "appliances" are connected and specify rights that are dependent on the determination.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
85. An electronic appliance at least temporarily connected to a rights authority broker, the electronic appliance receiving at least one rights context from the rights authority broker when the device is connected to the rights authority broker.	<i>See Claim 84 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
86. A method of defining at least one rights management context comprising:	<i>See Claim 84 above.</i>
(a) determining whether a first electronic appliance is present; and	<i>See Claim 84 above.</i>
(b) defining at least one rights management control set based at least in part on the determining step (a).	<i>See Claim 84 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
87. A method of defining at least one rights management context including:	<i>See Claim 84 above.</i>
(a) coupling an optical disk storing information to an electronic appliance that can be selectively connected to a rights management broker;	<i>See Claim 84 above.</i>
(b) determining whether the electronic appliance is currently coupled to a rights management broker; and	<i>See Claim 84 above.</i>
(c) conditioning at least one aspect of use of at least some of the information stored on the optical disk based on whether the electronic appliance is coupled to the rights management broker.	<i>See Claim 84 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
88. An electronic appliance including:	<i>See Claim 55 above.</i>
an optical disk reading and/or writing arrangement;	<i>See Claim 55 above.</i>
a secure node coupled to the optical disk reading and/or writing arrangement, the secure node performing at least one rights management related function with respect to at least some information read by the optical disk reading and/or writing arrangement; and	<i>See Claim 55 above.</i>
at least one serial bus port coupled to the secure node, the serial bus port for providing any or all of the functions, structures, protocols and/or methods of IEEE 1394-1995.	<ul style="list-style-type: none"> <li>• Applicants disclose that a data processor includes a display, a keyboard, a printer, a sound system, and other conventional means may be connected to a bus. (p.8, l.25-p.9, l.9; p.17, ll.1-12).</li> <li>• Thus, a "serial bus port coupled to the secure node" is inherently disclosed.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
89. A digital versatile disk appliance including:	<i>See</i> Claim 55 above.
means for watermarking content; and	<ul style="list-style-type: none"> <li>• Applicants disclose that the data object can consist of digital data, analog data or a combination or hybrid of analog and digital data. (p.4, ll.3-5).</li> <li>• Applicants disclose that security modules utilizing encryption algorithms and authorization processes may be used. (p.21, l.17-p.22, l.12).</li> <li>• Thus, means for watermarking information into the file is inherently disclosed.</li> </ul>
serial bus means for communicating the watermarked content,	<i>See</i> Claim 88 above.
wherein the serial bus means complies with IEEE 1394-1995.	<i>See</i> Claim 88 above.



<b>Copied Claim From Shear Appl. '077</b>	<b>Applicants' Disclosure</b>
90. An optical disk reading and/or writing device including:	<i>See Claim 88 above.</i>
at least one secure node capable of watermarking content and/or processing watermarked content; and	<i>See Claim 88 above.</i>
an IEEE 1394-1995 serial bus port.	<i>See Claim 88 above.</i>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>91. An optical disk using system and/or method including at least some of the elements shown in FIG. 1.</p>	<ul style="list-style-type: none"> <li>• This claim corresponds to Shear's claim 95 that refers to FIG. 3.</li> <li>• Applicants at least disclose a data object 24, control data, and secured data packages 40 in FIG. 1.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>92. An optical disk using system and/or method using at least some of the elements shown in FIG. 17.</p>	<ul style="list-style-type: none"> <li>• This claim corresponds to Shear's claim 96 that refers to FIG. 3A.</li> <li>• Applicants at least disclose an encrypted data package including data object(s) and control data.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>93. An optical disk using system and/or method using at least some of the control set elements shown in FIG. 8a.</p>	<ul style="list-style-type: none"> <li>• This claim corresponds to Shear's claim 97 that refers to FIG. 3B.</li> <li>• Applicants at least disclose an identifier, control data, and control elements.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>94. An optical disk using system and/or method using at least some of the elements shown in FIG. 15.</p>	<ul style="list-style-type: none"> <li>• This claim corresponds to Shear's claim 98 that refers to FIG. 4A.</li> <li>• Applicants at least disclose receiving a data package, a usage request, compliance with control conditions, and enabled usage.</li> </ul>



Copied Claim From Shear Appl. '077	Applicants' Disclosure
<p>95. In a network including at least one electronic appliance that reads information from and/or writes information to at least one digital versatile disk optical storage medium, and securely communicates information associated with at least one of payment, auditing, usage, access, controlling and/or otherwise managing content recorded on the storage medium, a method of processing said communicated information including the step of generating at least one payment request and/or order based at least in part on the information.</p>	<ul style="list-style-type: none"> <li>• See Claims 71 and 72 above.</li> <li>• Applicants disclose that managing of the broker-user business relationship and negotiating of the transaction between the broker and the user can be automated, and the control data structure can provide unlimited support to these operations. Payment for using a data object can be handled by transmitting credit card information, or the user can have a debit or credit account with the broker. (p.14, ll.24-30).</li> </ul>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
96. A method of authenticating a load module comprising:	Applicants disclose a method of authenticating data packages (p.21, ll.17-31).
(a) authenticating a first digital signature associated with the load module, including the step of employing a first one-way hash algorithm, a first decryption algorithm, and a first public key; and	<ul style="list-style-type: none"> <li>Applicants disclose the use of security modules that provide sophisticated encryption, authorization algorithms, access control, and usage control. (p.10, ll.1-4). Thus, the use of a hash algorithm is at least inherently disclosed.</li> <li>Applicants disclose the use of decryption modules. (p.18, ll.6-10).</li> <li>Applicants disclose the use of security modules including the use of public keys. (p.21, ll.17-31).</li> <li>Applicants disclose the use of extensible object security that may include multiple levels of security. (p.23, l.16-p.24, l.9).</li> </ul>
(b) authenticating a second digital signature associated with the load module, including the step of employing at least one of:	<ul style="list-style-type: none"> <li>Applicants disclose a method of authenticating data packages (p.21, ll.17-31).</li> <li>Applicants disclose the use of extensible object security that may include multiple levels of security. (p.23, l.16-p.24, l.9).</li> </ul>
(i) a second one-way hash algorithm that is dissimilar to the first one-way hash algorithm,	<ul style="list-style-type: none"> <li>See Claim 96(a) above.</li> </ul>
(ii) a second decryption algorithm that is dissimilar to the first decryption algorithm, and	Applicants disclose the use of decryption modules. (p.18, ll.6-10).
(iii) a second public key that is dissimilar to the first public key.	Applicants disclose the use of security modules including the use of public keys. (p.21, ll.17-31).



Copied Claim From Shear Appl. '072	Applicants' Disclosure
97. A protected processing environment comprising:	Applicants disclose a secure data processor (p.9, ll.8-9) including the use of passwords (p.18, ll.13-19).
means for providing a tamper resistant enclosure;	Applicants disclose the use of encryption modules, security modules, and passwords for providing a secure environment. (p.18, ll.1-5; p.18, ll.13-19).
means for maintaining at least one public verification key within the tamper resistant enclosure; and	Applicants disclose the use of security modules including the use of public keys with a secure data processor. (p.21, ll.17-31).
means for authenticating load modules based, at least in part, on use of the public verification key.	Applicants disclose the use of security modules including the use of public keys to authenticate data packages. (p.21, ll.17-31).



Copied Claim From Shear Appl. '072	Applicants' Disclosure
98. A method of distinguishing between trusted and untrusted load modules comprising:	Applicants disclose a method of authenticating data packages (p.21, ll.17-31).
(a) receiving a load module,	Applicants disclose a user receiving a data package. (p.19, ll.5-7; p.21, ll.24-26).
(b) determining whether the load module has an associated digital signature,	<ul style="list-style-type: none"> <li>Applicants disclose that the received data package is encrypted; in one example using RSA. (p.21, ll.18-20).</li> <li>Such encryption is recognized as applying a digital signature. <i>See e.g.</i>, Shear Pub. No. US 2001/0023214 A1, para. 93 ("Two digital signature algorithms in widespread use today [include] RSA and DSA").</li> </ul>
(c) if the load module has an associated digital signature, authenticating the digital signature using at least one secret public key; and	Applicants disclose the use of a public key to authenticate a data package. (p.21, ll.24-31).
(d) conditionally executing the load module based at least in part on the results of authenticating step (c).	Applicants disclose the use of a public key to enable usage of a data object. (p.21, ll.24-31).



Copied Claim From Shear Appl. '072	Applicants' Disclosure
<p>99. A method of increasing the security of a virtual distribution environment comprising plural interoperable protected processing environments having different work factors, the method comprising:</p>	<p>Applicants disclose the secure transfer of two different examples of data objects, a digital image (i.e., a first load module) and a video film (i.e., a second load module), requiring different security treatment with different security modules by a user's data processor prior to usage of the data objects (i.e., the plural protected processing environments have different work factors). (p.20, l.5-p.23, l.2).</p>
<p>(a) classifying the plural protected processing environments based on work factor,</p>	<p>Applicants disclose that usage control elements define a variety of usages of the data object, for example the kind of user, allowed operations, and security modules required for use of the data object on a user's data processor (i.e., classifying the processing environments based on work factor). (p.4, ll.11-19; p.18, ll.1-5).</p>
<p>(b) distributing different verification public keys to different protected processing environments having different work factor classifications, and</p>	<ul style="list-style-type: none"> <li>• See Claim 98(c) above and Claim 99(c) below.</li> </ul>



(c) using the distributed verification public keys to authenticate load modules, including the step of preventing protected processing environments having different work factor classifications from executing the same load module.

- See Claim 98(c) and 98(d) above.
- Applicants disclose that variation of object control can be applied to a particular object by creating a control data format with control elements defining the control variation and the circumstances in which the variation is applied. (p.23, ll.3-14).
- Applicants further disclose that variation of object security can be applied to a particular object by creating a control data format with control elements defining the security variation and the circumstances in which the variation is applied. (p.23, ll.16-29).
- Thus, it is at least inherent that control elements defining user type could include work factor classifications for the type of appliance.



Copied Claim From Shear Appl. '072	Applicants' Disclosure
100. A protected processing environment comprising:	Applicants disclose a secure data processor (p.9, ll.8-9) including the use of passwords (p.18, ll.13-19).
a tamper resistant barrier having a first work factor; and	Applicants disclose the use of encryption modules, security modules, and passwords for providing a secure environment. (p.18, ll.1-5; p.18, ll.13-19).
at least one arrangement within the tamper resistant barrier that prevents the protected processing environment from executing the same load module accessed by a further protected processing environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	<ul style="list-style-type: none"> <li>• See Claim 99(c) above.</li> <li>• Applicants disclose the use of security modules including the use of public keys to enable usage of data objects. (p.21, ll.17-31).</li> </ul>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
101. A method for protecting a computation environment surrounded by a tamper resistant barrier having a first work factor, the method including:	<i>See Claim 100 above.</i>
preventing the computation environment from using the same software module accessible by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	<ul style="list-style-type: none"> <li>• <i>See Claims 99(c) and 100 above.</i></li> </ul>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
102. A method of protecting computation environments comprising:	Applicants disclose a method of protecting computation environments.
(a) associating plural digital signatures with a load module;	<i>See</i> Claim 96(a) above.
(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and	<ul style="list-style-type: none"> <li>• Applicants disclose that object security can include multiple levels of security utilizing methods such as encryption and keys. (p.23, ll.26-29).</li> <li>• <i>See</i> Claims 96(a) and 99(c) above.</li> </ul>
(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.	<ul style="list-style-type: none"> <li>• Applicants disclose that object security can include multiple levels of security utilizing methods such as encryption and keys. (p.23, ll.26-29).</li> <li>• <i>See</i> Claims 96(b) and 99(c) above.</li> </ul>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
103. A computer security method comprising:	Applicants disclose that a general set of control data comprises a security control element which defines a security procedure which has to be carried out before usage of a data object. (p.4, ll.17-19).



digitally signing, using a first digital signing technique, a first executable designating the first executable for use by a first device class; and

- Applicants disclose encrypting (i.e., digitally signing) control elements and a data object (i.e., a first executable) (p.4, ll.27-28; p.12, ll.15-18) to create a secure data package ready for transfer to a user (p.5, ll.7-10). Applicants disclose that usage control elements define a variety of usages of the data object, for example the kind of user, allowed operations, and security modules required for use of the data object on a user's data processor (i.e., the digital signature designates the executable for use by a device class). (p.4, ll.11-15; p.18, ll.1-5).
- Applicants further disclose that the security of a data package can be improved by using a sophisticated encryption algorithm like RSA (p.21, ll.18-20) or other encryption and key methods (p.12, ll.15-18). Such usage is recognized as applying a digital signature. *See e.g.*, Shear Pub. No. US 2001/0023214 A1, para. 93 ("Two digital signature algorithms in widespread use today [include] RSA and DSA").
- Applicants disclose that the user's data processor is a general or special purpose processor (p.17, ll.2-3), data objects include books, films, video, news, music, software, games, etc. (p.2, ll.3-4), and the data object owner may want to have control over how, when, where, and by whom his property is used (p.2, ll.20-21). Applicants further disclose that object security is extensible in the sense that multiple levels of security can be applied, being dependent on the encryption/key method which is implemented in the security modules. (p.23, ll.26-29). Thus, Applicants disclose that a variety of data objects (i.e., executables) can be designated for use by data processors having certain required security modules (i.e., a device class).
- Therefore, Applicants disclose digitally signing (i.e., encrypting) a first executable (i.e., a data object such as a digital image or a video file) with a first digital signature designating the first executable for use by a first device class (i.e., the encrypted control/usage elements require the user's data processor to have certain required security modules in order to use the data object).



digitally signing, using a second digital signing technique different from the first digital signing technique, a second executable designating the second executable for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class.

- See above regarding digitally signing an executable and designating a device class.
- See also Claim 96(a) above regarding a second digital signing technique.
- Applicants disclose the secure transfer of two different examples of data objects, a digital image (i.e., a first executable) and a video film (i.e., a second executable), requiring different security treatment with different security modules by a user's data processor prior to usage of the data objects (i.e., designating executables for use by devices having different tamper resistance and/or work factors). (p.20, l.5-p.23, l.2).
- Applicants disclose that the general set of control data associated with a data object comprises an identifier, which uniquely identifies the general set of control data. The whole set of control data and the data object may be encrypted (i.e., digital signature of a second executable can be different from a digital signature of a first executable). (p.4, ll.19-28).
- Applicants disclose that a user program comprising a usage manager module controls the usage of a data object in accordance with the control data. The user program comprises one or more security modules (i.e., user device level of security, or user device tamper resistance and/or work factor). (p.17, ll.15-20). The usage manager module applies the security modules which are necessary to use a data object. If the proper security modules are not available for a particular data object, the usage manager module will not permit usage of the data object (i.e., a second device class may have a tamper resistance and/or work factor different from the tamper resistance and/or work factor of the first device class). (p.18, ll.1-5).
- Therefore, Applicants disclose digitally signing a second executable (e.g., a video file or a digital image) with a second digital signature different from the first digital signature (i.e., encrypted unique control data), the second digital signature designating the second executable for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class (i.e., encrypted control/usage elements can require the user's data processor to have different security modules in order to use different data objects).



Copied Claim From Shear Appl. '072	Applicants' Disclosure
104. A method of authenticating an executable comprising:	<ul style="list-style-type: none"> <li>• See Claim 96 above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(a) authenticating a first digital signature associated with the executable, including the step of employing a first one-way hash algorithm, a first decryption algorithm, and a first public key; and	<ul style="list-style-type: none"> <li>• See Claim 96(a) above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(b) authenticating a second digital signature associated with the executable, including the step of employing at least one of:	<ul style="list-style-type: none"> <li>• See Claim 96(b) above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(i) a second one-way hash algorithm that is dissimilar to the first one-way hash algorithm,	See Claim 96(b)(i) above.
(ii) a second decryption algorithm that is dissimilar to the first decryption algorithm, and	See Claim 96(b)(ii) above.
(iii) a second public key that is dissimilar to the first public key.	See Claim 96(b)(iii) above.



Copied Claim From Shear Appl. '072	Applicants' Disclosure
105. A secure execution space comprising:	<i>See Claim 97 above.</i>
means for providing a tamper resistant barrier;	<ul style="list-style-type: none"> <li>• <i>See Claim 97 above.</i></li> <li>• A "tamper resistant barrier" is inherent in a "tamper resistant enclosure."</li> </ul>
means for maintaining at least one public verification key within the tamper resistant barrier; and	<ul style="list-style-type: none"> <li>• <i>See Claim 97 above.</i></li> <li>• A "tamper resistant barrier" is inherent in a "tamper resistant enclosure."</li> </ul>
means for authenticating executables based, at least in part, on use of the public verification key.	<i>See Claim 97 above.</i>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
106. A method of distinguishing between trusted and untrusted executables comprising:	<ul style="list-style-type: none"> <li>• See Claim 98 above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(a) receiving an executable;	<ul style="list-style-type: none"> <li>• See Claim 98(a) above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(b) determining whether the executable has an associated digital signature;	<ul style="list-style-type: none"> <li>• See Claim 98(b) above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(c) if the executable has an associated digital signature, authenticating the digital signature using at least one secret public key; and	<ul style="list-style-type: none"> <li>• See Claim 98(c) above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(d) conditionally executing the executable based at least in part on the results of authenticating step (c).	<ul style="list-style-type: none"> <li>• See Claim 98(d) above.</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
107. A method of increasing the security of plural interoperable secure execution spaces having different work factors, the method comprising:	<ul style="list-style-type: none"> <li>• See Claim 99 above.</li> <li>• A "secure execution space" is equivalent to a "protected processing environment."</li> </ul>
(a) classifying the plural secure execution spaces based on work factor;	<ul style="list-style-type: none"> <li>• See Claim 99(a) above.</li> <li>• A "secure execution space" is equivalent to a "protected processing environment."</li> </ul>
(b) distributing different verification public keys to different secure execution spaces having different work factor classifications; and	<ul style="list-style-type: none"> <li>• See Claim 99(b) above.</li> <li>• A "secure execution space" is equivalent to a "protected processing environment."</li> </ul>
(c) using the distributed verification public keys to authenticate executables, including the step of preventing secure execution spaces having different work factor classifications from executing the same executable.	<ul style="list-style-type: none"> <li>• See Claim 99(c) above.</li> <li>• An "executable" is equivalent to a "load module."</li> <li>• A "secure execution space" is equivalent to a "protected processing environment."</li> </ul>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
108. A protected processing environment comprising:	<i>See Claim 100 above.</i>
a tamper resistant barrier having a first work factor; and	<i>See Claim 100 above.</i>
at least one arrangement within the tamper resistant barrier that prevents the secure execution space from executing the same executable accessed by a further secure execution space having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	<ul style="list-style-type: none"> <li>• <i>See Claim 100 above.</i></li> <li>• A "secure execution space" is equivalent to a "protected processing environment."</li> <li>• An "executable" is equivalent to a "load module."</li> </ul>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
109. A method for protecting a computation environment surrounded by	<i>See Claim 101 above.</i>
a tamper resistant barrier having a first work factor, the method including:	<i>See Claim 101 above.</i>
preventing the computation environment from using the same software module accessed by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	<i>See Claim 101 above.</i>



Copied Claim From Shear Appl. '072	Applicants' Disclosure
110. A method of protecting computation environments comprising:	<i>See Claim 102 above.</i>
(a) associating plural digital signatures with an executable;	<ul style="list-style-type: none"> <li>• <i>See Claim 102(a) above.</i></li> <li>• An "executable" is equivalent to a "load module."</li> </ul>
(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and	<i>See Claim 102(b) above.</i>
(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.	<i>See Claim 102(c) above.</i>



Copied Claim From Ginter Appl. '806	Applicants' Disclosure
111. A rights management appliance including:	Applicants disclose a data processor (i.e., an appliance) to be used for managing data objects (i.e., for rights management). (p.8, l.25-p.9, l.9; p.17, ll.1-12).
a user input device,	Applicants disclose a keyboard (i.e., a user input device). (p.9, l.1; FIG.2).
a user display device,	Applicants disclose a display (i.e., a user display device). (p.9, l.1; FIG.2).
at least one processor, and	Applicants disclose a data processor including a CPU (i.e., a processor). (p.8, ll.29-30).
at least one element defining a protected processing environment,	<ul style="list-style-type: none"> <li>• Applicants disclose a user program including a decryption module and one or more security modules (i.e., at least one element) operably coupled to a user's data processor. (p.17, ll.15-20). If the proper format and security modules are not available for a particular data object, usage is not permitted (i.e., a protected processing environment). (p.18, ll.3-5).</li> <li>• The user program can have code which controls use of the program by password. (p.18, ll.13-14).</li> <li>• The data object is never stored in native format in user accessible storage. (p.18, ll.22-24).</li> <li>• Applicants disclose that the data provider's data processor is considered secure. (p.9, ll.8-9).</li> </ul>



characterized in that the protected processing environment stores and uses permissions, methods, keys, programs and/or other information to electronically manage rights.	Applicants disclose that a user/data provider's data processor utilizes control data, security modules including keys, decryption modules, and programs (i.e., permissions, methods, keys, programs, and/or other information) to control the usage of a data object (i.e., electronically manages rights). (p.17, ll.15-20; p.21, l.17-p.22, l.12)
---	---



<b>Copied Claim From Ginter Appl. '806</b>	<b>Applicants' Disclosure</b>
112. In a rights management appliance including:	<i>See Claim 111 above.</i>
a user input device,	<i>See Claim 111 above.</i>
a user display device,	<i>See Claim 111 above.</i>
at least one processor, and	<i>See Claim 111 above.</i>
at least one element defining a protected processing environment,	<i>See Claim 111 above.</i>
a method of operating the appliance characterized by the step of storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.	<i>See Claim 111 above.</i>



Copied Claim From Ginter Appl. '806	Applicants' Disclosure
<p>113. A rights management appliance including at least one processor element at least in part defining a protected processing environment, characterized in that the protected processing environment stores and uses permissions, methods, keys, programs and/or other information to electronically manage rights.</p>	<p><i>See Claim 111 above.</i></p>



Copied Claim From Ginter Appl. '806	Applicants' Disclosure
<p>114. In a rights management appliance including at least one processor element at least in part defining a protected processing environment, a method comprising storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.</p>	<p><i>See Claim 111 above.</i></p>



Copied Claim From Ginter Appl. '806	Applicants' Disclosure
<p>115. An electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, said arrangement including means to monitor usage of at least one aspect of an amount of appliance usage and control said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.</p>	<ul style="list-style-type: none"> <li>• See Claim 111 above.</li> <li>• Applicants disclose at least a database 20 for control data. (p.9, ll.6-7).</li> <li>• Applicants further disclose that a security module may implement an authorization process, according to which each usage of the data object requires a dial up to the data processor of the data object provider. (p.22, ll.1-12; p.23, l.29-p.24, l.2).</li> <li>• Applicants disclose the "control data structure can include control elements for complex user types, usage types . . ." (i.e., appliance usage). "Security modules could require a dial up to the brokers data processor to approve loading or usage actions . . ." (p.25, ll.8-13).</li> </ul>



Copied Claim From Ginter Appl. '806	Applicants' Disclosure
<p>116. In an electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, a method characterized by the steps of monitoring usage of at least one aspect of appliance usage and controlling said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.</p>	<p><i>See Claim 115 above.</i></p>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
117. A secure component-based operating process including:	Applicants disclose the handling of composite data objects (e.g., software) (i.e., component-based processes). (p.24, 1.11-p.25, 1.3).
(a) retrieving at least one component;	<ul style="list-style-type: none"> <li>Applicants disclose the use or formation of composite objects comprising constituent objects (i.e., one component). (p.24, 11.12-14).</li> <li>Furthermore, Applicants disclose buy and sell order packages (i.e., at least one component) are received by a stock trading data processor (pp.26-27).</li> </ul>
(b) retrieving a record that specifies a component assembly;	<ul style="list-style-type: none"> <li>Applicants disclose utilizing a control data format with control elements defining relationships between constituent objects and defining a parent/child element (i.e., a record that specifies component assembly). (p.24, 11.12-14).</li> <li>Furthermore, Applicants disclose the buy and sell order packages each include control data for a match (i.e., a record that specifies component assembly).</li> </ul>
(c) checking said component and/or said record for validity;	<ul style="list-style-type: none"> <li>Applicants disclose that a general set of control data comprises a security control element which defines a security procedure which has to be carried out before usage of a data object. (p.4, 11.17-19).</li> <li>The "security" disclosed by Applicants relates generally to "encryption" methods and "authorization" algorithms (e.g., RSA and key methods) (i.e., checking said component and/or said record for validity). (p.21, 11.17-31).</li> </ul>



<p>(d) using said component to form said component assembly in accordance with said record; and</p>	<ul style="list-style-type: none"> <li>• Applicants disclose combining data objects to create a new data object created with control data linking the constituent data objects (i.e., using said component to form said component assembly). (p.24, ll.27-30).</li> <li>• Applicants disclose a broker who can include a video (i.e., a component) and text book (i.e., a component) in an educational package (i.e., assembly). (p.24, ll.11-31).</li> <li>• Furthermore, Applicants disclose a match between the buy and sell order packages results in a transfer of digital money with repackaged and updated data packages (i.e., component assembly). (p.26, l.29-p.27, l.2).</li> </ul>
<p>(e) performing a process based at least in part on said component assembly.</p>	<ul style="list-style-type: none"> <li>• Applicants disclose that a general set of control data is created for a composite data object that can be distributed by a broker to a user. (p.24, ll.11-31).</li> <li>• Applicants disclose enabling data object usage and limiting the number of usages based upon control data (i.e., performing a process based at least in part on said component assembly). (p.19, ll.26-30).</li> <li>• Furthermore, Applicants disclose the new data packages after a match are transferred back to the seller and buyer data processors (i.e., performing a process). (pp.26-27)</li> </ul>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
118. A secure component operating system process including:	<i>See Claim 117 above.</i>
receiving a component;	<i>See Claim 117(a) above.</i>
receiving directions specifying use of said component to form a component assembly;	<i>See Claim 117(b) above.</i>
authenticating said received component and/or said directions;	<i>See Claim 117(c) above.</i>
forming, using said component, said component assembly based at least in part on said received directions; and	<i>See Claim 117(d) above.</i>
using said component assembly to perform at least one operation.	<i>See Claim 117(e) above.</i>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
119. A method comprising performing the following steps within a secure operating system environment:	Applicants disclose that the user's data processor is a secure processor (p.9, ll.8-9) requiring certain security modules for usage of the data object (i.e., a secure operating system environment. (p.18, ll.3-5).
providing code;	Applicants disclose providing of a data object, which can include software (i.e., code). (p.2, l.3).
providing directions specifying assembly of said code into an executable program;	See Claim 117(b) above.
checking said received code and/or said assembly directions for validity; and	See Claim 117(c) above.
in response to occurrence of an event, assembling said code in accordance with said received assembly directions to form an assembly for execution.	<ul style="list-style-type: none"> <li>• Applicants disclose that in response to an authorization to use (i.e., an event), a user may access a data object. (p.5, ll.25-30; p.19, ll.20-25).</li> <li>• A data object may include composite data objects. Constituent data objects may be combined to create a composite data object (i.e., an assembly) for some particular use, created with control data linking the constituent data objects (i.e., assembling said code in accordance with received assembly instructions). (p.24, ll.27-30).</li> </ul>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
<p>120. A method for managing at least one resource with a secure operating environment, said method comprising:</p>	<ul style="list-style-type: none"> <li>• Applicants disclose management of data objects for distribution by an author, broker, or user (i.e., a resource). (p.1, ll.14-16; p.8, ll.26-29; p.14, ll.25-30).</li> <li>• Applicants disclose a secure operating environment. <i>See</i> Claim 119 above.</li> </ul>
<p>securely receiving a first control from a first entity external to said operating environment;</p>	<ul style="list-style-type: none"> <li>• Applicants disclose usage conditions with a data object (i.e., a first control) from an author (i.e., a first entity) may be sent to a broker's data processor (i.e., operating environment). (p.8, ll.9-17).</li> <li>• Applicants disclose buy and sell order with control data are received by a stock trading data processor. (pp.26-27).</li> </ul>
<p>securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;</p>	<ul style="list-style-type: none"> <li>• Applicants disclose a broker may repackage a received data object and add further control data (i.e., a second control) which is relevant to his business activities. (p.8, ll.9-17).</li> <li>• Applicants further disclose a broker may combine constituent data objects into a composite data object for distribution. (p.24, ll.11-24).</li> <li>• Thus, it is at least inherent that a second data object with a second set of control data from a different author than the first could be sent to a broker's data processor.</li> <li>• Applicants disclose the buy and sell control data are sent from two different entities. (pp.26-27).</li> </ul>



securely processing, using at least one resource, a data item associated with said first and second controls; and	<ul style="list-style-type: none"> <li>• Applicants disclose a broker including a video data object and a text book data object in an educational package (i.e., a data item). (p.24, ll.12-19).</li> <li>• <i>See Claim 117(e) above.</i></li> <li>• Applicants further disclose that the buy and sell order control data are used in conjunction to transfer digital money (i.e., a data item). (pp.26-27).</li> </ul>
securely applying said first and second controls to manage said resource for use with said data item.	Applicants disclose a broker adding program procedures to program modules to process the control elements of constituent objects. (p.24, ll.12-19).



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
121. A method for securely managing at least one operation on a data item performed at least in part by an electronic arrangement, said method comprising:	Applicants disclose management of data objects (i.e., data items) for distribution by a broker, agent, or user (i.e., by an electronic arrangement – agreements between participants in a commercial value chain and/or a data security chain model for handling, auditing, reporting, and payment). (p.1, ll.14-16; p.8, ll.26-29; p.14, ll.25-30).
(a) securely delivering a first procedure to said electronic arrangement;	Applicants disclose usage conditions (i.e., a first procedure) from an author may be sent to a broker's data processor with a data object. (p.8, ll.9-17).
(b) securely delivering, to said electronic arrangement, a second procedure separable or separate from said first procedure;	<ul style="list-style-type: none"> <li>Applicants disclose a broker may repackage a received data object and add further control data (i.e., a second procedure) which is relevant to his business activities. (p.8, ll.9-17).</li> <li>Applicants further disclose a broker may combine constituent data objects with constituent control data into a composite data object for distribution. Each constituent data object retains its original control data which continues to control its subsequent usage. (p.24, ll.11-31).</li> <li>Thus, it is at least inherent that a second data object with a second set of control data (i.e., a second procedure) may be delivered to a broker's data processor.</li> <li>Furthermore, Applicants disclose that a user requests authorization (i.e., a second procedure) to use a data object. (p.5, ll.25-30; p.19, ll.8-12).</li> <li>Applicants further disclose two different sets of control data (buy and sell orders) are sent to a stock trading data processor. (pp.26-27).</li> </ul>



<p>(c) performing at least one operation on said data item, including using said first and second procedures in combination to at least in part securely manage said operation; and</p>	<ul style="list-style-type: none"> <li>• Applicants disclose enabling data object usage and limiting the number of usages based upon control data. (p.19, ll.26-30).</li> <li>• Applicants further disclose that a usage manager module compares the user request for usage with the corresponding control data (i.e., using said first and second procedures in combination). If the requested usage is not permitted in the control data, the requested usage is disabled. (p.19, ll.20-25).</li> <li>• See Claims 117(e) and 120 above.</li> <li>• Applicants further disclose that the buy and sell order control data are used in conjunction to transfer digital money (i.e., a data item). (pp.26-27).</li> </ul>
<p>(d) securely conditioning at least one aspect of use of said data item based on said delivering steps (a) and (b) having occurred.</p>	<ul style="list-style-type: none"> <li>• It is inherent that if a user does not request usage, no use of the data object will occur.</li> <li>• Applicants also disclose an automated transaction negotiation in which digital money is not transferred without a matching of a delivered sell order and a delivered buy order. (pp.26-27).</li> </ul>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
122. A method for securely managing at least one operation performed at least in part by a secure electronic appliance, comprising:	Applicants disclose management of data objects using data processors including security modules (i.e., a secure electronic appliance). (p.8, 1.25-p.9, 1.9).
(a) selecting an item that is protected with respect to at least one operation;	See Claim 121(c) above.
(b) securely independently delivering plural separate procedures to said electronic appliance;	See Claim 121(a) and 121(b) above.
(c) using said plural separate procedures in combination to at least in part securely manage said operation with respect to said selected item; and	See Claims 117(e) and 121(c) above.
(d) conditioning successful completion of said operation on said delivering step (b) having occurred.	See Claim 121(d) above.



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
123. A method for processing based on independent deliverables comprising:	<i>See Claim 117 above.</i>
securely delivering a first piece of code defining a first part of a process;	<i>See Claims 120 and 121(a) above.</i>
separately, securely delivering a second piece of code defining a second part of said process;	<i>See Claims 120 and 121(b) above.</i>
ensuring the integrity of the first and second delivered pieces of code; and	<i>See Claim 117(c) above.</i>
performing said process based at least in part on said first and second delivered code pieces.	<i>See Claims 117(e) and 120 above.</i>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
124. A method of securely controlling at least one protected operation with respect to a data item comprising:	<i>See Claim 121(c) above.</i>
(a) supplying at least a first control from a first party;	<i>See Claims 120 and 121(a) above.</i>
(b) supplying at least a second control from a second party different from said first party;	<i>See Claims 120 and 121(b) above.</i>
(c) securely combining said first and second controls to form a set of controls;	<i>See Claims 117(d), 117(e), and 120 above.</i>
(d) securely associating said control set with said data item; and	<i>See Claim 117(d) and 117(e) above.</i>
(e) securely controlling at least one protected operation with respect to said data item based on said control set.	<i>See Claims 120 and 121(c) above.</i>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
125. A secure method for combining data items into a composite data item comprising:	Applicants disclose the handling of composite data objects including constituent data objects. (p.24, ll.11-24).
(a) securely providing a first data item having at least a first control associated therewith;	<i>See Claims 117(a), 120, and 121(a) above.</i>
(b) securely providing a second data item having at least a second control associated therewith;	<i>See Claims 120 and 121(b) above.</i>
(c) forming a composite of said first and second data items;	<i>See Claim 117(d) above.</i>
(d) securely combining said first and second controls into a composite control set; and	<i>See Claim 117(e) above.</i>
(e) performing at least one operation on said composite of said first and second data items based at least in part on said composite control set.	<i>See Claim 117(e) above.</i>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
126. A secure method for controlling a protected operation comprising:	<i>See</i> Claim 121 above.
(a) delivering at least a first control and a second control; and	<i>See</i> Claims 120, 121(a), and 121(b) above.
(b) controlling at least one protected operation based at least in part on a combination of said first and second controls, including at least one of the following steps:	<i>See</i> Claim 121(c) above.
resolving at least one conflict between said first and second controls based on a predefined order,	<ul style="list-style-type: none"> <li>• Applicants disclose matching and non-matching between two sets of buy and sell control data (i.e., resolving conflict based on a predefined order). (pp.26-27).</li> <li>• Applicants disclose a composite object can be handled by defining a control data format with control elements defining relationships between constituent objects and by defining a parent/child element. (p.24, ll.12-14).</li> <li>• It is also at least inherent in the formation of composite objects that conflicts between the control data of the constituent objects will be resolved based on a predefined order.</li> </ul>
providing an interaction with a user to form said combination; and	Applicants disclose a user can combine data objects for some particular purpose. (p.24, ll.27-31). <i>See also</i> Claim 117(d) above.
dynamically negotiating between said first and second controls.	Applicants disclose an automated transaction negotiation method between two sets of control data. (pp.26-27).



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
127. A secure method comprising:	Applicants disclose a secure method.
selecting protected data;	<ul style="list-style-type: none"> <li>• Applicants disclose data objects protected in a package. (p.9, ll.12-14).</li> <li>• Furthermore, Applicants disclose digital money (i.e., protected data) in a buy and sell negotiation. (pp.26-27).</li> </ul>
extracting said protected data from an object;	<ul style="list-style-type: none"> <li>• Applicants disclose a user extracting protected data from a data package. (p.19, ll.20-28).</li> <li>• Furthermore, Applicants disclose that the user program executes a transaction whereby the digital money (i.e., protected data) is extracted from the buy order data package and transferred to the sell order package. (p.26, l.29-p.27, l.2).</li> </ul>
identifying at least one control to manage at least one aspect of use of said extracted data;	<ul style="list-style-type: none"> <li>• Applicants disclose control data associated with a constituent data object and control data associated with a composite data object. (p.24, ll.20-31; FIG. 17).</li> <li>• Furthermore, Applicants disclose the control data of the sell order data package (i.e., at least one control) is updated after the matching of buy and sell orders and transfer of digital money (i.e., extracted data). (pp.26-27).</li> </ul>
placing said extracted data into a further object; and	<ul style="list-style-type: none"> <li>• Applicants disclose creating a parent object with constituent objects and combining data objects. (p.24, ll.12-31).</li> <li>• Furthermore, Applicants disclose transfer of digital money to the sell order package (i.e., a further object). (pp.26-27).</li> </ul>



associating said at least one control with said further object.

- Applicants disclose control data associated with a constituent data object and control data associated with a composite data object. (p.24, ll.20-31; FIG. 17).
- Control elements may define relationships between constituent objects and a parent/child relationship. (p.24, ll.12-14).
- Furthermore, Applicants disclose the control data of the sell order data package (i.e., at least one control) is updated after the matching of buy and sell orders and transfer of digital money (i.e., extracted data). (pp.26-27).



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
128. A secure method of modifying a protected object comprising:	Applicants disclose combining data objects to create a new data object (i.e., a protected object is modified). (p.24, ll.27-31).
(a) providing a protected object; and	Applicants disclose protected data objects.
(b) embedding at least one additional element into said protected object without unprotecting said object.	Applicants disclose combining data objects to form a new data object (i.e., embedding an element into the protected object) with control data linking the constituent data objects. Each constituent data object retains its original control data which continues to control its subsequent usage. (p.24, ll.12-31).



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
129. A method for managing at least one resource with a secure operating environment, said method comprising:	<i>See Claim 120 above.</i>
securely receiving a first load module from a first entity external to said operating environment;	<ul style="list-style-type: none"> <li>• <i>See Claim 120 above.</i></li> <li>• A "load module" is equivalent to a "control".</li> </ul>
securely receiving a second load module from a second entity external to said operating environment, said second entity being different from said first entity;	<ul style="list-style-type: none"> <li>• <i>See Claim 120 above.</i></li> <li>• A "load module" is equivalent to a "control".</li> </ul>
securely processing, using at least one resource, a data item associated with said first and second load modules; and	<ul style="list-style-type: none"> <li>• <i>See Claim 120 above.</i></li> <li>• A "load module" is equivalent to a "control".</li> </ul>
securely applying said first and second load modules to manage said resource for use with said data item.	<ul style="list-style-type: none"> <li>• <i>See Claim 120 above.</i></li> <li>• A "load module" is equivalent to a "control".</li> </ul>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
130. A method for negotiating electronic contracts, comprising:	Applicants disclose an automated transaction negotiation. (pp.26-27).
receiving a first control set from a remote site;	Applicants disclose a seller/buyer that creates control data, e.g. kind of stock, price, quantity (i.e., a first control set) on the seller's/buyer's data processor (i.e., a remote site) to participate in a negotiation. The rules or conditions for buying and selling stocks are indicated in the control data. (p.26).
providing a second control set;	Applicants disclose a buyer's/seller's control data (i.e., a second control set).
performing, within a protected processing environment, an electronic negotiation between said first control set and said second control set, including providing interaction between said first and second control sets; and	<ul style="list-style-type: none"> <li>Applicants disclose performing automated negotiations at the data processor of the stock trading company (i.e., a protected processing environment). (p.27, ll.3-4).</li> <li>Applicants disclose that the control data of the sell (i.e., first control set) and buy (i.e., second control set) order packages are examined and matched (i.e., providing interaction between said first and second control sets) by the user program of the stock trading company. (p.26, ll.27-29).</li> </ul>
producing a negotiated control set resulting from said interaction between said first and second control sets.	Applicants disclose that the user program executes a transaction, whereby digital money is extracted from the buy order data package and transferred to the sell order package. Then the control data of the sell order data package is updated (i.e., producing a negotiated control set) after the matching of buy and sell orders (i.e., as a result of an interaction between the first control set and the second control set). (p.26, l.29-p.27, l.2).



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
131. A system for supporting electronic commerce including:	Applicants disclose an electronic system for supporting a broker-user business relationship (i.e., electronic commerce). (p.14, ll.26-29).
means for creating a first secure control set at a first location;	<ul style="list-style-type: none"> <li>Applicants disclose a data provider (e.g., an author) may secure control data with a data object on the data provider's data processor (i.e., first location) including a data packaging program (i.e., means for creating a first secure control set). (p.11, l.21-p.12, l.22).</li> <li><i>See also</i> Claims 130 above and 132 below.</li> </ul>
means for creating a second secure control set at a second location;	<ul style="list-style-type: none"> <li>Applicants disclose a broker may repackage a received data package and add further control data (i.e., a second secure control set) which is relevant to his business activities with a data packaging program on the broker's data processor (i.e., means at a second location). (p.8, ll.9-16; p.8, l.25-p.10, l.14).</li> <li><i>See also</i> Claims 130 above and 132 below.</li> </ul>
means for securely communicating said first secure control set from said first location to said second location; and	<ul style="list-style-type: none"> <li>Applicants disclose an author may provide a data object in a secure package from the author's data processor (i.e., first location) including network and telecommunications programs (i.e., means for communicating) to a broker's data processor (i.e., second location). (p.8, ll.9-16; p.8, l.25-p.9, l.9).</li> <li><i>See also</i> Claims 130 above and 132 below.</li> </ul>



means at said second location for securely integrating said first and second control sets to produce at least a third control set comprising plural elements together comprising an electronic value chain extended agreement.

- Applicants disclose a broker may create a parent composite object with control elements referring to constituent objects (i.e., first and second control sets) and the parent object (i.e., a third control set). (p.24, ll.11-26; FIG. 17).
- *See also* Claims 130 above and 132 below.



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
132. A system for supporting electronic commerce including:	<i>See Claim 131 above.</i>
means for creating a first secure control set at a first location;	Applicants disclose a buyer that creates control data, e.g. kind of stock, price, quantity (i.e., a first secure control set) on the buyer's data processor (i.e., a first location). (p.26).
means for creating a second secure control set at a second location;	Applicants disclose a seller that creates control data, e.g. kind of stock, price, quantity (i.e., a second secure control set) on the seller's data processor (i.e., a second location). (p.26).
means for securely communicating said first secure control set from said first location to said second location; and	<ul style="list-style-type: none"> <li>• Applicants disclose a buyer's control data being sent to a stock trading company (p.26). It is inherent that a buyer's control data could be sent to a seller's data processor or vice versa.</li> <li>• Also, Applicants disclose an author may provide a data object in a secure package from the author's data processor (i.e., first location) including network and telecommunications programs (i.e., means for communicating) to a broker's data processor (i.e., second location). (p.8, ll.9-16; p.8, l.25-p.9, l.9).</li> </ul>
negotiation means at said second location for negotiating an electronic contract through secure execution of at least a portion of said first and second secure control sets.	<ul style="list-style-type: none"> <li>• Applicants disclose performing automated negotiations at the data processor of the stock trading company. (p.27, ll.3-4). Upon identifying matched buy and sell orders, the user program executes a transaction. (p.26, ll.29-30).</li> <li>• Thus, it is at least inherent that negotiations can occur at the seller's data processor.</li> </ul>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
133. A secure component-based operating system including:	<i>See</i> Claim 117 above.
component retrieving means for retrieving at least one component;	<ul style="list-style-type: none"> <li>• <i>See</i> Claim 117(a) above.</li> <li>• Applicants disclose a file transfer program that can transfer and receive files via a network to and from other data processors. (p.18, ll.25-26; FIG.14).</li> </ul>
record retrieving means for retrieving a record that specifies a component assembly;	<ul style="list-style-type: none"> <li>• <i>See</i> Claim 117(b) above.</li> <li>• Applicants disclose a usage manager module that calls 1) a decryption module that decrypts and extracts control data from a data package and 2) a control data parser module to extract data fields from usage elements (i.e., record retrieving means). (p.19, ll.13-19; FIG.14).</li> </ul>
checking means, coupled to said component retrieving means and said record retrieving means, for checking said component and/or said record for validity;	<ul style="list-style-type: none"> <li>• <i>See</i> Claim 117(c) above.</li> <li>• Applicants disclose decryption modules and security modules (i.e., checking means) that apply access control and verification using encryption/key methods such as RSA. (p.17, ll.27-29; p.21, ll.17-31; FIG.14).</li> </ul>
using means, coupled to said checking means, for using said component to form said component assembly in accordance with said record; and	<ul style="list-style-type: none"> <li>• <i>See</i> Claim 117(d) above.</li> <li>• Applicants disclose a usage manager module that unpackages and enables data object usage. (p.19, ll.13-28; FIG.14).</li> </ul>



performing means, coupled to said using means, for performing a process based at least in part on said component assembly.

- See Claim 117(e) above.
- Applicants disclose a user program (i.e., performing means) that controls the usage of a data object in accordance with the control data included in the data package together with the data object. (p.17, ll.15-16; FIG.14).



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
134. A secure component-based operating system including:	<i>See Claims 117 and 133 above.</i>
a database manager that retrieves, from a secure database, at least one component and at least one record that specifies a component assembly;	<ul style="list-style-type: none"> <li>• <i>See Claims 117(a) and 133 above.</i></li> <li>• Applicants disclose a memory that can store a received data package and a database intended for control data. (p.17, ll.9-12).</li> </ul>
an authenticating manager that checks said component and/or said record for validity;	<i>See Claims 117(c) and 133 above.</i>
a channel manager that uses said component to form said component assembly in accordance with said record; and	<i>See Claims 117(d) and 133 above.</i>
an execution manager that performs a process based at least in part on said component assembly.	<i>See Claims 117(e) and 133 above.</i>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
135. A secure component operating system including:	<i>See Claims 117 and 133-134 above.</i>
means for receiving a component;	<i>See Claims 117(a) and 133-134 above.</i>
means for receiving directions specifying use of said component to form a component assembly;	<i>See Claims 117(b) and 133 above.</i>
means, coupled to said receiving means, for authenticating said received component and/or said directions;	<i>See Claims 117(c) and 133-134 above.</i>
means, coupled to said authenticating means, for forming, using said component, said component assembly based at least in part on said received directions; and	<i>See Claims 117(d) and 133-134 above.</i>
means, coupled to said forming means, for using said component assembly to perform at least one operation.	<i>See Claims 117(e) and 133-134 above.</i>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
136. A secure component operating environment including:	<i>See Claims 117 and 133-135 above.</i>
a storage device that stores a component and directions specifying use of said component to form a component assembly;	<i>See Claims 117(a) and 133-135 above.</i>
an authenticating manager that authenticates said component and/or said directions;	<i>See Claims 117(c) and 133-135 above.</i>
a channel manager that forms, using said component, said component assembly based at least in part on said directions; and	<i>See Claims 117(d) and 133-135 above.</i>
a channel that executes said component assembly to perform at least one operation.	<i>See Claims 117(e) and 133-135 above.</i>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
137. A secure operating system environment comprising:	<i>See Claims 117 and 133-136 above.</i>
a storage device that stores code and directors specifying assembly of said code into an executable program;	<i>See Claims 117(a) and 133-136 above.</i>
a validating device that checks said received code and/or said assembly directors for validity; and	<i>See Claims 117(c) and 133-136 above.</i>
an event-driven channel that, in response to occurrence of an event, assembles said code in accordance with said assembly directions to form an assembly for execution.	<i>See Claims 117(d), 119, and 133-136 above.</i>



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
138. A secure operating environment system for managing at least one resource comprising:	<ul style="list-style-type: none"> <li>• See Claim 120 above.</li> <li>• Applicants disclose a secure data processor. See Claim 119 above.</li> </ul>
a communications arrangement that securely receives a first control from a first entity external to said operating environment, and securely receives a second control from a second entity external to said operating environment, said second entity being different from said first entity; and	<ul style="list-style-type: none"> <li>• See Claims 120 and 131-137 above.</li> <li>• Applicants disclose network and telecommunications programs between authors and brokers and between buyers, sellers, and stock trading companies.</li> </ul>
a protected processing environment, coupled to said communications arrangement, that:	<ul style="list-style-type: none"> <li>• See Claims 120 and 131-137 above.</li> <li>• Applicants disclose secure data processors.</li> </ul>
(a) securely processes, using at least one resource, a data item associated with said first and second controls, and	See Claims 120 and 131-137 above.
(b) securely applies said first and second controls to manage said resource for use of said data item.	See Claims 120 and 131-137 above.



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
139. A system for negotiating electronic contracts, comprising:	<i>See Claims 131-138 above.</i>
a storage arrangement that stores a first control set received from a remote site, and stores a second control set;	<i>See Claims 131-138 above.</i>
a protected processing environment, coupled to said storage arrangement, that:	<i>See Claims 131-138 above.</i>
(a) performs an electronic negotiation between said first control set and said second control set,	<i>See Claims 131-138 above.</i>
(b) provides interaction between said first and second control sets, and	<i>See Claims 131-138 above.</i>
(c) produces a negotiated control set resulting from said interaction between said first and second control sets.	<i>See Claims 131-138 above.</i>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
140. A method for supporting electronic commerce including:	<i>See Claims 130-132 above.</i>
creating a first secure control set at a first location;	<i>See Claims 130-132 above.</i>
creating a second secure control set at a second location;	<i>See Claims 130-132 above.</i>
securely communicating said first secure control set from said first location to said second location; and	<i>See Claims 130-132 above.</i>
electronically negotiating, at said second location, an electronic contract, including the step of securely executing at least a portion of said first and second secure control sets.	<i>See Claims 130-132 above.</i>



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
141. An electronic appliance comprising:	Applicants disclose an electronic appliance. (p.17, ll.1-12).
a processor; and	Applicants disclose a data processor with a CPU. (p.17, ll.2-3).
at least one memory device connected to said processor;	Applicants disclose memory connected to a processor. (p.17, ll.4-12; FIG.13).
wherein said processor includes:	
retrieving means for retrieving at least one component, and at least one record that specifies a component assembly, from said memory device,	See Claims 117(b) and 133-137 above.
checking means coupled to said retrieving means for checking said component and/or said record for validity, and	See Claims 117(c) and 133-137 above.
using means coupled to said retrieving means for using said component to form said component assembly in accordance with said record.	See Claims 117(d) and 133-137 above.



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
142. An electronic appliance comprising:	<i>See Claim 141 above.</i>
at least one processor;	<i>See Claim 141 above.</i>
at least one memory device connected to said processor; and	<i>See Claim 141 above.</i>
at least one input/output connection coupled to said processor,	Applicants disclose that a display, a keyboard, a printer, a sound system, a ROM, and a bulk storage device may be connected to a bus connected to the CPU. (p.17, ll.1-12).
wherein said processor at least in part executes a rights operating system to provide a secure operating environment within said electronic appliance.	Applicants disclose a user program that controls the usage of a data object (i.e., a rights operating system). The user program is executed by the user's secure data processor. (p.17, ll.15-16; p.19, ll.5-7).



<b>Copied Claim From Ginter Appl. '370</b>	<b>Applicants' Disclosure</b>
143. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:	Applicants disclose sending of audit-like information related to use of a resource.
securely receiving a first control from a first entity external to said operating environment;	<i>See Claims 120 and 130-132 above.</i>
securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;	<i>See Claims 120 and 130-132 above.</i>
using at least one resource;	<i>See Claims 120 and 130-132 above.</i>



securely sending to said first entity in accordance with said first control, first audit information concerning use of said resource; and

- Applicants disclose that one level of security for a broker may be to require on-line confirmation when loading a data object to the user's data processor to permit the broker to check that the object has not already been loaded as well as to double check all other parameters (i.e., audit report). (p.23, 1.29-p.24, 1.2). Furthermore, Applicants disclose that security modules could require a dial up to the brokers data processor to approve loading or usage actions and to implement approval authentication mechanisms. (p.25, 11.11-13).
- Thus, it is at least inherent that audit information, like a usage request, could be sent to a broker/data object provider upon use of a data object.
- Applicants disclose that a copy of a user set of control data is preferably stored in the broker's control database to provide a record with which to compare subsequent use, e.g., when a dial-up is required for usage. Thus, it is inherent that either control data is equivalent to audit information or that a broker/agent provides a two-way conduit for rights and audit data between content creators and content users.
- Applicants also disclose that the control data of both buy and sell order packages are updated to provide an audit trail after the transaction and transferred back to their authors (i.e., sending of audit information concerning use). (pp.26-27).

securely sending to said second entity in accordance with said second control, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

*Id. See above.*



Copied Claim From Ginter Appl. '370	Applicants' Disclosure
144. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:	<i>See Claims 120 and 143 above.</i>
securely receiving first and second control alternatives from an entity external to said operating environment;	<ul style="list-style-type: none"> <li>Applicants disclose receiving buy and sell order controls, which may not match, at a stock trading company's data processor. (p.26)</li> </ul>
selecting one of said first and second control alternatives;	<ul style="list-style-type: none"> <li>Applicants disclose either matching or not matching buy and sell order controls, which is equivalent to selecting one of the control alternatives.</li> </ul>
using at least one resource;	<i>See Claim 143 above.</i>
if said first control alternative is selected by said selecting step, securely sending to said entity in accordance with said first control alternative, first audit information concerning use of said resource; and	<i>See Claims 120 and 143 above.</i>
if said second control alternative is selected by said selecting step, securely sending to said second entity in accordance with said second control alternative, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.	<i>See Claims 120 and 143 above.</i>



<b>Copied Claim From Ginter '140</b>	<b>Applicants' Disclosure</b>
145. A method for automated negotiation, including the following steps:	Applicants disclose an automated transaction negotiation. (p.26-27).
creating a first rule set at a first site, the first rule set designed to participate in an automatic negotiation with a second rule set;	Applicants disclose a seller that creates control data, e.g. kind of stock, price, quantity (i.e., a first rule set) on the seller's data processor (i.e., a first site) to participate in a negotiation with a buyer's control data (i.e., a second rule set). The rules or conditions for buying and selling stocks are indicated in the control data. (p.26).
transmitting the first rule set from the first site to a second site,	Applicants disclose that the sell order package containing the seller's control data (i.e., the first rule set) is transferred from the seller's data processor (i.e., the first site) to the data processor of the stock trading company (i.e., a second site), where it is received and stored in the memory. (p.26, ll.25-27).
at the second site, performing an automated negotiating process including:	Applicants disclose performing automated negotiations at the data processor of the stock trading company (i.e., the second site). (p.27, ll.3-4).
comparing information present in or specified by the first rule set to a first requirement specified by a second rule set present at the second site;	Applicants disclose that the control data of the sell (i.e., first rule set) and buy (i.e., second rule set) order packages are examined and matched (i.e., information from rule sets are compared) by the user program of the stock trading company (i.e., at the second site). (p.26, ll.27-29).
if the comparison results in a first outcome, carrying out a first action, the first action including:	Applicants disclose that upon identifying matched buy and sell orders (i.e., comparison results in a first outcome), the user program executes a transaction (i.e., a first action). (p.26, ll.29-30).



creating a secure container consisting of protected content and having an associated third rule set, the third rule set being created as a result of an interaction between the first rule set and the second rule set;	<ul style="list-style-type: none"> <li>Applicants disclose that the user program executes a transaction, whereby the digital money (i.e., protected content) is extracted from the buy order data package and transferred to the sell order package. Then the control data of the sell order data package is updated (i.e., to create a third rule set) and repackaged (i.e., to create a secure container) after the matching of buy and sell orders (i.e., as a result of an interaction between the first rule set and the second rule set). (p.26, l.29-p.27, l.2).</li> </ul>
transmitting the secure container from the second site to the first site; and	Applicants disclose that the new sell order package containing the digital money (i.e., the secure container) is transferred from the data processor of the stock trading company (i.e., the second site) back to the seller's data processor (i.e., the first site). (p.27, ll.1-2).
using a rule from the third rule set to govern an aspect of access to or use of the protected content; and	Applicants disclose that control data (i.e., the third rule set) controls access to and the usage of the data object (i.e., the protected content). (p.10, ll.12-13; p.19, ll.20-25).
if the comparison results in a second outcome, carrying a second action, which is different in at least one respect from the first action.	<ul style="list-style-type: none"> <li>Applicants disclose that upon identifying matched buy and sell orders the user program executes a transaction.</li> <li>It is at least inherent that without a match, no transaction takes place (i.e., a second action, which is different in at least one respect from the first action).</li> <li>Compare to Ginter '140, col.246, l.38-col.247, l.38 (disclosing different types of negotiation to form an electronic contract, including a demand by one party to form an "adhesion" type contract and more complex forms of negotiation analogous to "haggling."</li> </ul>



<b>Copied Claim From Ginter '140</b>	<b>Applicants' Disclosure</b>
146. A method for automated negotiation, including the following steps:	<i>See Claim 145 above.</i>
creating a first rule set at a first site;	<ul style="list-style-type: none"> <li>• <i>See Claim 145 above.</i></li> <li>• Seller's data processor is disclosed as a "first site."</li> </ul>
creating a second rule set at a second site;	<ul style="list-style-type: none"> <li>• <i>See Claim 145 above.</i></li> <li>• Buyer's data processor is disclosed as a "second site."</li> </ul>
transmitting the first rule set from the first site to a third site;	<ul style="list-style-type: none"> <li>• <i>See Claim 145 above.</i></li> <li>• Stock trading company's data processor is disclosed as a "third site."</li> </ul>
transmitting the second rule set to the third site;	<i>See Claim 145 above.</i>
at the third site, performing the following steps:	<i>See Claim 145 above.</i>
comparing a requirement specified by the first rule set to a requirement specified by the second rule set and determining that the requirements are consistent;	<i>See Claim 145 above.</i>



based at least in part on the results of the comparison, creating a third rule set, the third rule set including at least one rule specified at least in part by the first rule set and the second rule set;	<ul style="list-style-type: none"> <li>• See Claim 145 above regarding “third rule set.”</li> <li>• Applicants disclose that control data is updated to provide an audit trail by reflecting the author/user(broker) or seller/buyer relationships. (p.16, ll.26-29). In other words, the updated control data is a third rule set that includes “at least one rule specified at least in part by the first rule set and the second rule set.”</li> <li>• Furthermore, Applicants disclose composite objects and a combining usage action: a content owner may want to sell composite objects with different rules governing each constituent object (p.2, ll.24-26; p.24, ll.20-22), and a new data object can be created by a combination of data objects with control data linking the constituent data objects and each constituent data object retaining its original control data. (p.24, ll.28-31). When a user requests authorization for usage of one constituent data object in a composite data object, a user set of control data is created only for that constituent data object and packaged only with a copy of that constituent data object. (p.25, ll.1-3).</li> <li>• Thus, it is at least inherent that composite sell or buy order data packages could be used for combinations between the data packages to create a third data package containing a “third rule set including at least one rule specified at least in part by the first rule set and the second rule set.”</li> </ul>
associating the third rule set with a secure container;	See Claim 145 above.
encapsulating protected content into the secure container; and	See Claim 145 above.



transmitting the secure container to the  
first site.

*See Claim 145 above.*



Copied Claim From Ginter '140	Applicants' Disclosure
147. A method for automated negotiation including the following steps:	<i>See Claims 145-146 above.</i>
generating a first rule set including a first rule from a first party which owns or at least in part controls governed content and a second rule from a second party which constitutes or includes a clearinghouse;	<ul style="list-style-type: none"> <li>• <i>See Claims 145-146 above.</i></li> <li>• Applicants disclose a content author as a party which owns or at least in part controls governed content and generates a first control data (i.e., a first party).</li> <li>• Applicants disclose an "agent (broker)" or "distributor". It is at least inherent that an "agent (broker)" includes a "clearinghouse."</li> <li>• Applicants disclose that a broker may apply his own usage conditions (i.e., a second rule from a second party) to a data packaging program by adding further control data which is relevant to his business activities in addition to the author's control data (i.e., a first rule from a first party). (p.8, ll.13-17). Thus, a data package may include a first rule set of control data from multiple parties, including from the content author (i.e., a first party) and the broker (i.e., a second party).</li> <li>• Furthermore, Applicants disclose a sell order package including control data (i.e., a first rule from a first party) is sent to a stock trading company, similar to a clearinghouse, which may add its own rules (i.e., a second rule from a second party) to make a first rule set.</li> </ul>
incorporating the governed content into a secure container;	<i>See Claims 145-146 above.</i>
storing the first rule set at a first site;	Applicants disclose a broker's data processor as a first site.



transmitting a second rule set from a second site to the first site, the second rule set including a third rule from a third party;	<ul style="list-style-type: none"> <li>• Applicants disclose a buyer's request (i.e., a third rule from a third party), which may be transmitted from the buyer's data processor (i.e., a second site) to the broker's data processor (i.e., the first site).</li> <li>• Furthermore, Applicants disclose a buy order package (i.e., a second rule set including a third rule from a third party).</li> </ul>
comparing at least a portion of the first rule set to at least a portion of the second rule set; and	<i>See Claims 145-146 above.</i>
based on the results of the comparison, providing access to the secure container to the third party.	<i>See Claims 145-146 above.</i>



<b>Copied Claim From Ginter '140</b>	<b>Applicants' Disclosure</b>
148. A method of automated negotiation including:	<i>See Claims 145-147 above.</i>
creating a first rule set representing a negotiating position of a first party;	<i>See Claims 145-147 above.</i>
incorporating the first rule set into a first secure container;	Applicants disclose a seller (i.e., a first party) that incorporates associated control data, e.g. kind of stock, price, quantity (i.e., a first rule set) into a secure package (i.e., a first secure container). (p.26, ll.21-24)
creating a second rule set representing a negotiating position of a second party;	<i>See Claims 145-147 above.</i>
incorporating the second rule set into a second secure container;	Applicants disclose a buyer (i.e., a second party) that incorporates associated control data, e.g. kind of stock, price, quantity (i.e., a second rule set) into a secure package (i.e., a second secure container). (p.26, ll.21-24)
selecting a negotiation site associated with a third party;	<ul style="list-style-type: none"> <li>• <i>See Claims 145-147 above.</i></li> <li>• The stock trading company's data processor is disclosed as a "negotiation site associated with a third party."</li> </ul>
transmitting the first and the second secure containers to the negotiation site;	Applicants disclose that the sell and buy order packages (i.e., the first and the second secure containers) are transferred to the data processor of the stock trading company (i.e., the negotiation site), where they are received and stored in the memory. (p.26, ll.25-27).



at the negotiation site, comparing an attribute of the first rule set to an attribute of the second rule set to determine whether the attributes are compatible and, depending on the results of the comparison, determining that the negotiation has succeeded, determining that the negotiation has failed, or determining that an additional comparison is required;	<ul style="list-style-type: none"> <li>• See Claims 145-147 above regarding “a first action” and “a second action” (i.e., determining that the negotiation has succeeded or failed).</li> <li>• Applicants disclosure of automated “negotiation” at least inherently includes “determining that an additional comparison is required.”</li> </ul>
if the negotiation has succeeded, transmitting a third secure container to the first party, the third secure container containing governed content;	<ul style="list-style-type: none"> <li>• Applicants disclose that the user program executes a transaction upon identifying matched sell and buy orders, (i.e., if the negotiation has succeeded), whereby the digital money (i.e., governed content) is extracted from the buy order data package and transferred to the sell order package.</li> <li>• The control data of the sell order data package is updated and repackaged and sent back to the seller’s data processor (i.e., a third secure container is created and transmitted to the first party). (p.26, 1.29-p.27, 1.2).</li> </ul>
if the negotiation has failed, informing both parties of the failure, and not transmitting the third secure container to the first party; and	<ul style="list-style-type: none"> <li>• Applicants disclose that an audit trail is made by informing the parties of a match and that a third secure data package is transmitted upon the match. (p.26-27).</li> <li>• Thus, it is at least inherent that the parties could be informed of a non-match (i.e., informing parties of the failure) or that no return of the data packages is “informing both parties of the failure.”</li> </ul>
if an additional comparison is required, performing that comparison, and repeating until the negotiation either succeeds or fails.	Applicants disclosure of a “negotiation” process involving the matching of two sets of rules or conditions at a stock trading company at least inherently includes “repeating until the negotiation either succeeds or fails.”



Copied Claim From Ginter '402	Applicants' Disclosure
149. A method including:	Applicants disclose a method.
creating a first secure container including a first governed item and having associated a first control;	<ul style="list-style-type: none"> <li>• Applicants disclose a seller that creates a secure package (i.e., a first secure container) comprising an empty data file (i.e., a first governed item) and associated control data, e.g. kind of stock, price, quantity (i.e., a first control). (p.26, ll.21-24).</li> <li>• Furthermore, Applicants disclose a content author that creates a data package (i.e., a first secure container) including a data object (i.e., a first governed item) and associated control data (i.e., a first control). <i>See Claims 145-148 above.</i></li> </ul>
creating a second secure container including a second governed item and having associated a second control;	<ul style="list-style-type: none"> <li>• Applicants disclose a buyer that creates a secure package (i.e., a second secure container) comprising a digital money data file (i.e., a second governed item) and associated control data, e.g. kind of stock, price, quantity (i.e., a second control). (p.26, ll.17-20).</li> <li>• <i>See above regarding "content author that creates a data package."</i></li> <li>• <i>See Claims 145-148 above.</i></li> </ul>



transferring the first secure container from a first location to a second location;	<ul style="list-style-type: none"> <li>Applicants disclose that the sell order package (i.e., the first secure container) is transferred from the seller's data processor (i.e., a first location) to the data processor of the stock trading company (i.e., a second location), where it is received and stored in the memory. (p.26, ll.25-27).</li> <li>Furthermore, Applicants disclose a content author may transfer the author's data package to a broker (i.e., a second location). <i>See</i> Claims 145-148 above.</li> </ul>
transferring the second secure container from a third location to the second location;	<ul style="list-style-type: none"> <li>Applicants disclose that the buy order package (i.e., the second secure container) is transferred from the buyer's data processor (i.e., a third location) to the data processor of the stock trading company (i.e., a second location), where it is received and stored in the memory. (p.26, ll.25-27).</li> <li>Furthermore, Applicants disclose a content author may transfer the author's data package to a broker (i.e., the second location). <i>See</i> Claims 145-148 above.</li> </ul>
at the second location, obtaining access to at least a portion of the first governed item, the access being governed at least in part by the first control;	<ul style="list-style-type: none"> <li>Applicants disclose that the user program of the stock trading company (i.e., at the second location) examines the control data of the sell order package (i.e., the first control) and looks for a match. Upon identifying matched buy and sell orders, the user program executes a transaction, whereby the digital money is extracted from the buy order data package and transferred to the sell order package (i.e., access is obtained to at least a portion of the first governed item). (p.26, ll.27-31).</li> <li>Furthermore, Applicants disclose a broker obtaining access to at least a portion of the content from the authors with access being controlled by control data. (p.8, ll.9-17).</li> </ul>



at the second location, obtaining access to at least a portion of the second governed item, the access being governed at least in part by the second control;

- Applicants disclose that the user program of the stock trading company (i.e., at the second location) examines the control data of the buy order package (i.e., the second control) and looks for a match. Upon identifying matched buy and sell orders, the user program executes a transaction, whereby the digital money is extracted from the buy order data package (i.e., access is obtained to at least a portion of the second governed item) and transferred to the sell order package. (p.26, ll.27-31).
- Furthermore, Applicants disclose a broker obtaining access to at least a portion of the content from the authors with access being controlled by control data. (p.8, ll.9-17).



at the second location, creating a third secure container including at least a portion of the first governed item and at least a portion of the second governed item and having associated at least one control, the creation being governed at least in part by the first control and the second control.

- Applicants disclose that the user program (i.e., at the second location) executes a transaction upon identifying matched sell and buy orders, (i.e., being governed at least in part by the first control and the second control), whereby the digital money (i.e., at least a portion of the second governed item) is extracted from the buy order data package, transferred to the sell order package (i.e., at least a portion of the first governed item), and the control data of the sell order data package is updated (i.e., at least one control) and repackaged (i.e., a third secure container is created). (p.26, l.29-p.27, l.2).
- Furthermore, Applicants disclose composite objects and a combining usage action: a content owner or broker may want to sell composite objects with different rules governing each constituent object (p.2, ll.24-26; p.24, ll.20-22), and a new data object can be created by a combination of data objects with control data linking the constituent data objects. (p.24, ll.28-31). When a user requests authorization for usage of one constituent data object in a composite data object, a user set of control data is created only for that constituent data object and packaged only with a copy of that constituent data object. (p.25, ll.1-3).
- Thus, it is at least inherent that composite sell or buy order data packages could be used for combinations between the data packages to create a third data package (i.e., a third secure container). Also, Applicants disclose a broker selling composite objects (i.e., a third secure container).



Copied Claim From Ginter '488	Applicants' Disclosure
150. A method of using a resource including the following steps:	<ul style="list-style-type: none"> <li>• Applicants disclose a method of distributing a data object, which includes books, films, video, news, music, software, games, etc. (i.e., a resource). (p.2, ll.2-3).</li> <li>• Compare to Ginter '488, col.7, ll.49-61 (A resource refers to information that may be distributed, such as software programming resources and reference/record keeping information resources (such as business, medical, legal, scientific, governmental, and consumer databases)).</li> </ul>
receiving the resource at a first computing environment;	<ul style="list-style-type: none"> <li>• In a first example, Applicants disclose distributing a data object (i.e., resource) by a broker or electronic bulletin board (i.e., a first computing environment). (p.14, l.25-p.16, l.29; p.20, ll.9-10).</li> <li>• In a second example, Applicants disclose a data package including content (i.e., resource) is received by a user's data processor (i.e., a first computing environment).</li> <li>• In a third example, Applicants disclose computer automated stock trading with buy and sell orders containing digital money (i.e., resource) at a stock trading company (i.e., a first computing environment). (p.26).</li> </ul>



<p>receiving a first control or control set at the first secure computing environment;</p>	<p>In the first example and second examples, Applicants disclose the content author and/or broker may package the data object with corresponding usage conditions or control data (i.e., first control or control set). (p.8, ll.9-17).</p> <ul style="list-style-type: none"> <li>• In the third example, Applicants disclose a sell order with control data, e.g., kind of stock, price, quantity (i.e., first control or control set). (p.26).</li> </ul>
<p>receiving a second control or control set at the first secure computing environment;</p>	<ul style="list-style-type: none"> <li>• In the first example, Applicants disclose that when a request for authorization for usage is received, a user set of control data (i.e., second control or control set) is created by the data provider's processor. (p.4, l.31-p.5, l.1; p.15, ll.4-5).</li> <li>• In the first and second examples, Applicants disclose variable and extensible object control in which variation of object control (i.e., a second control or control set) can be applied to a particular object by creating a control data format with control elements defining the control variation and the circumstances in which the variation is applied. (p.23, ll.5-14).</li> <li>• In the third example, Applicants disclose a buy order with control data, e.g., kind of stock, price, quantity (i.e., second control or control set). (p.26).</li> </ul>



evaluating an auditing-related aspect of the first control or control set and the second control or control set, including evaluating a privacy-related aspect of the first control or control set and the second control or control set;

- In the first example, Applicants disclose that a data program compares (i.e., evaluates) a usage request from a user (i.e., second control or control set) with the usage control elements of the control data of the data object (i.e., first control or control set) to see if the usage request complies with the predetermined conditions for usage indicated therein. The comparison may include comparing the user type, the usage type, the number of usages, the price, identification, billing address, etc. (i.e., auditing-related aspect and privacy-related aspect) (p.15, ll.6-10; p.20, ll.25-28).
- In the second example, Applicants disclose evaluating control variation and the circumstances in which the variation is applied. (p.23, ll.5-14).
- In the third example, Applicants disclose the user program of the stock trading company examines the control data of the buy and sell order packages and looks for a match (i.e., evaluates the first and second controls or control sets). (p.26).
- Compare Ginter '488, col.247, ll.9-33 (In a scenario for purchasing information in which the price paid depends on the amount of information about the user that is returned along with a usage audit trail, content users can evaluate the amount of privacy-related information provided to the content provider) and Ginter '488, col.43, ll.63-67 (A user might require a method that summarizes usage information for reporting to a clearinghouse (e.g. billing information) in a way that does not convey confidential, personal information regarding detailed usage behavior).



choosing between the first control or control set and the second control or control set, the choice being based at least in part on the evaluation; and

- In the first example, Applicants disclose that if the requested usage complies with the predetermined conditions (i.e., choice is based at least in part on the evaluation) the authorization is granted (i.e., second control or control set chosen), otherwise it is rejected (i.e., first control or control set chosen).
- In the second example, Applicants disclose a choice between control variations based upon evaluation of circumstances (p.23, ll.5-14).
- In the third example, Applicants disclose that upon identifying matched buy and sell order the user program executes a transaction (i.e., chooses between the first control or control set and the second control or control set). (p.26).
- Compare to Ginter '488, col.294, ll.19-27 (End users may transmit permissions and/or other control information to the repository permitting and/or denying access to usage information collected by the audit system for use by the analysis system).
- Compare to Ginter '488, col.247, ll.12-18 (The right to use the content may be associated with two control sets. One control set may describe a fixed ("higher") price for using the content. Another control set may describe a fixed ("lower") price for using the content with additional control information and field specifications requiring collection and return of the user's personal information).
- Compare to Ginter '488, col.248, ll.13-18 (The content creator may "prefer" one of the two control sets over the other one. If so, the preferred control set may be "offered" first in the negotiation process, and withdrawn in favor of the non-preferred control set if the other party to the negotiation "rejects" the preferred control set).



reporting auditing-related information relating to the access to or use of the resource to a second computing environment.

- In the first example, it is inherent that a broker/agent provides a two-way conduit for rights and audit data between content creators and content users.
- In the second example, Applicants disclose that one level of security for a broker may be to require on-line confirmation when loading a data object to the user's data processor to permit the broker to check that the object has not already been loaded as well as to double check all other parameters (i.e., audit report). (p.23, 1.29-p.24, 1.2).
- In the third example, Applicants disclose that the control data of both the buy and sell order packages are updated to provide an audit trail after the transaction and transferred back to their authors (i.e., information relating to the access to or use of the resource is reported to a second computing environment). (p.26-27).
- Compare to Ginter '488, col.293, ll.26-32 (Audit information related to usage of content can be processed and passed to a billing system and/or transmitted to appropriate content authors).



Pursuant to 37 C.F.R. §§ 1.604 and 1.607, Applicants propose at this time that each of the claims being copied be deemed a count for the purposes of provoking an interference. However, we reserve the right to alter the counts if necessary.

The present application was filed on August 21, 2003 as a continuation of U.S. Patent Application No. 09/321,386 filed May 27, 1999, which in turn claimed priority to U.S. Patent Application No. 09/164,606, filed October 1, 1998, which in turn claimed priority to U.S. Patent Application No. 08/594,811, filed on January 31, 1996, now U.S. Patent No. 5,845,281, which in turn claimed priority to Swedish Application No. 9500355-4, filed on February 1, 1995. The present application is based on substantially the same disclosure as U.S. Patent Application No. 08/594,811, now U.S. Patent No. 5,845,281, which contained substantially the same disclosure as in Swedish Application No. 9500355-4. Thus, Claims 54-150 are supported by the disclosure of Swedish Application No. 9500355-4 and is entitled to a priority date of February 1, 1995.

The aforementioned Claim 54 is copied from U.S. Patent No. 6,292,569, issued to Shear et al. on September 18, 2001 as a continuation of U.S. Patent Application No. 08/689,754, filed on August 12, 1996, now U.S. Patent No. 6,157,721. Thus, because the present application has a priority date of over 1.5 years prior to the priority date of Shear '569, Applicants allege that based upon priority of invention, Applicants are entitled to a judgment relative to the patentee of Shear '569.

35 U.S.C. § 135(b) does not bar this copied claim because the claim was filed in parent U.S. Patent Application No. 09/321,386 on September 18, 2002, within twelve months of the issuance date of the target patent, September 18, 2001.

The aforementioned Claims 55-95 are copied from U.S. Patent Application No. 08/848,077, Publication No. 2001/0042043, published on November 15, 2001 for Shear as a continued prosecution application with a parent application filed on May 15, 1997. Thus, because the present application has a priority date earlier than the priority date of Shear Appl. '077, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the applicants of Shear Appl. '077.



35 U.S.C. § 135(b) does not bar these copied claims because the claims were filed in parent U.S. Patent Application No. 09/321,386 on November 14, 2002, within twelve months of the publication date of the target patent application, November 15, 2001.

The aforementioned Claims 96-110 are copied from U.S. Patent Application No. 09/925,072, Publication No. 2002/0023214, published on February 21, 2002 for Shear as a continuation of U.S. Patent Application No. 09/678,830, filed on October 4, 2000, now U.S. Patent No. 6,292,569, which is a continuation of U.S. Patent Application No. 08/689,754, filed on August 12, 1996, now U.S. Patent No. 6,157,721. Thus, because the present application has a priority date earlier than the priority date of Shear Appl. '072, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the applicants of Shear Appl. '072.

35 U.S.C. § 135(b) does not bar these copied claims because the claims were filed in parent U.S. Patent Application No. 09/321,386 on February 21, 2003, within twelve months of the publication date of the target patent application, February 21, 2002.

The aforementioned Claims 111-116 are copied from U.S. Patent Application No. 09/948,806, Publication No. 2002/0048369, published on April 25, 2002 for Ginter et al. as a division of U.S. Patent Application No. 09/272,998, filed on March 19, 1999, which is a continuation of U.S. Patent Application No. 08/706,208, filed on August 30, 1996, now abandoned. Thus, because the present application has a priority date earlier than the priority date of Ginter Appl. '806, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the inventors of Ginter Appl. '806.

35 U.S.C. § 135(b) does not bar these copied claims because the claims were filed in parent U.S. Patent Application No. 09/321,386 on March 26, 2003, within twelve months of the publication date of the target patent application, April 25, 2002.

The aforementioned Claims 117-144 are copied from U.S. Patent Application No. 09/764,370, Publication No. 2002/0112171, published on August 15, 2002 for Ginter et al. as a continuation of U.S. Patent Application No. 09/335,465, filed on June 17, 1999, now U.S. Patent No. 6,237,786, which is a continuation of U.S. Patent Application No. 08/780,393, filed on January 8, 1997, now U.S. Patent No. 5,915,019, which is a division of U.S. Patent Application No. 08/388,107, filed on February 13, 1995, now abandoned. Thus, because the



present application has a priority date earlier than the priority date of Ginter Appl. '370, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the inventors of Ginter Appl. '370.

35 U.S.C. § 135(b) does not bar these copied claims because the claims were filed in parent U.S. Patent Application No. 09/321,386 on March 26, 2003, within twelve months of the publication date of the target patent application, August 15, 2002.

The aforementioned Claims 145-148 are copied from U.S. Patent No. 6,427,140, issued to Ginter et al. on July 30, 2002 as a continuation of U.S. Patent Application No. 08/778,256, filed on January 8, 1997, now U.S. Patent No. 5,949,876, which is a division of U.S. Patent Application No. 08/388,107, filed on February 13, 1995, now abandoned. Thus, because the present application has a priority date earlier than the priority date of Ginter '140, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the patentee of Ginter '140.

35 U.S.C. § 135(b) does not bar these copied claims because the claim was filed in parent U.S. Patent Application No. 09/321,386 on March 26, 2003, within twelve months of the issuance date of the target patent, July 30, 2002.

The aforementioned Claim 149 is copied from U.S. Patent No. 6,389,402, issued to Ginter et al. on May 14, 2002 as a continuation of U.S. Patent Application No. 08/964,333, filed on November 4, 1997, now U.S. Patent No. 5,982,891, which is a continuation of U.S. Patent Application No. 08/388,107, filed on February 13, 1995, now abandoned. Thus, because the present application has a priority date earlier than the priority date of the patentee, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the patentee of Ginter '402.

35 U.S.C. § 135(b) does not bar this copied claim because the claim was filed in parent U.S. Patent Application No. 09/321,386 on March 26, 2003, within twelve months of the issuance date of the target patent, May 14, 2002.

The aforementioned Claim 150 is copied from U.S. Patent No. 6,363,488, issued to Ginter et al. on March 26, 2002 as a continuation of U.S. Patent Application No. 08/760,440, filed on December 4, 1996, now U.S. Patent No. 5,910,987, which is a continuation of U.S. Patent Application No. 08/388,107, filed on February 13, 1995, now abandoned. Thus, because



the present application has a priority date earlier than the priority date of the patentee, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the patentee of Ginter '488.

35 U.S.C. § 135(b) does not bar this copied claim because the claim was filed in parent U.S. Patent Application No. 09/321,386 on March 26, 2003, within twelve months of the issuance date of the target patent, March 26, 2002.



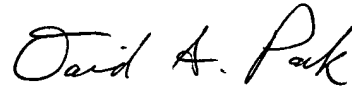
**CONCLUSION**

Accordingly, Applicants respectfully request that an interference be declared between the present Applicants and inventors of the aforementioned patents and applications. If there are any questions, please do not hesitate to call the undersigned at (949) 752-7040.

Express Mail Label No.:

EV 252 520 090US

Respectfully submitted,



David S. Park  
Attorney for Applicant(s)  
Reg. No. 52,094